CONFIDENTIALITY
COALITION

General Committee Meeting
Thursday, September 24, 2020
3:00pm – 4:00pm
https://zoom.us/j/99014143254?pwd=YWZyTFd4UmYvR0g2U1ZTdDZPeTlndz09
Meeting ID: 990 1414 3254
Password: 301302

1. Welcome and Introductions

2. Guest Speaker — Attachment 1
   Alice Leiter, Vice President and General Counsel, eHealth Initiative

3. eHI and CDT Draft Privacy Framework for Consumer Health Data — Attachment 2, 3

4. Regulatory Update — Attachment 4, 5
   a. HIPAA Coordinated Care Proposed Rule
   b. HIPAA Plasma Donation Guidance
   c. ONC Information Blocking Interim Final Rule

5. Legislative Update — Attachment 6, 7
   a. SAFE DATA Act
   b. California Consumer Privacy Act Revisions

6. Monthly Privacy Round Up — Attachment 8

7. Articles of Interest — Attachment 9, 10, 11

Attachment #1

Alice Leiter

Vice President & General Counsel, eHealth Initiative

Alice is a health regulatory lawyer with a specialty in health information privacy law and policy. She previously worked as a Senior Associate at the law firm Hogan Lovells, where she worked with clients on Medicare and Medicaid pricing and reimbursement. Alice spent several years as policy counsel at two different non-profit organizations, the National Partnership for Women & Families and the Center for Democracy & Technology. She currently sits on the DC HIE Policy Board, as well as the boards of Beauvoir School, Educare DC, and DC Greens, the latter of which she chairs. She received her B.A. in human biology from Stanford University and her J.D. from the Georgetown University Law Center. Alice and her husband, Michael, live in Washington, D.C. with their four children.

Attachment #2

Proposed Consumer Privacy Framework for Health Data

Draft for Public Feedback

August 26, 2020

eHealth Initiative

Center for Democracy and Technology

Attachment #2

Table of Contents

Attachment #2

Background

Health data — or data used for health-related purposes — is not regulated by a single national privacy framework. Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has governed the use and disclosure of certain health information held by certain entities like doctors and insurance companies. However, with the rise of wearable devices, health and wellness apps, online services, and the Internet of Things (IoT), extraordinary amounts of information reflecting mental and physical wellbeing are created and held by entities who are not bound by HIPAA obligations. This issue has only gained importance in the last several months, as new regulations will also be moving HIPAA-covered medical records into this commercially-facing and unregulated space. The novel coronavirus, too, has thrust the issue of patient data privacy to the forefront, as efforts to trace and combat the spread of the virus has brought with it the relaxation of some federal privacy protections, as well as increased data collection and use.

Project Goals and Status

With funding from the Robert Wood Johnson Foundation, the eHealth Initiative (eHI) and the Center for Democracy & Technology (CDT) have been collaborating on a Consumer Privacy Framework for Health Data, with invaluable engagement and help from a Steering Committee of leaders from healthcare providers, technology companies, academia, and organizations advocating for privacy, consumer, and civil rights. Two workgroups – focused on the Framework's Substance and Structure – have developed detailed use, access, and disclosure principles and controls for health data designed to address the gaps in legal protections for health data outside HIPAA's coverage, along with a draft self-regulatory model to support enforcement of such standards. The standards' emphasis is on transparency, accountability, and the limitation on health data collection, disclosure, and use. Importantly, the standards:

(1) move beyond outdated notice and consent models,

(2) cover all health information, and

(3) cover all entities that use, disclose or collect consumer health information, regardless of the size or business model of the covered entity.

This proposal is not designed to be a replacement for necessary comprehensive data privacy legislation. Given that Congressional action to pass such a law is likely some time away, this effort is designed to build consensus on best practices and to do what we can now, in the interim, to shore up protections for non-HIPAA covered health data.

Attachment #2

Value of this Proposal

Consumers. This model raises the bar for consumer privacy. Some existing best practices or voluntary frameworks define health information quite narrowly, and do not cover all of the data that reflects mental or physical wellbeing or health. Many best practices are also often targeted at a specific type of app or service instead of all entities that collect and use health data. Our comprehensive proposal closes these gaps in coverage.

Substantively, our draft goes beyond outdated models that revolve primarily around notice and consent. While such laws or frameworks may have made sense in decades past, people can no longer make informed and timely decisions about all the different websites, apps, and devices they use everyday. By putting clear restrictions on the collection, use, and sharing of data, the draft shifts the burden of privacy risk off of users.

Finally, because our model borrows the best concepts from Europe and California, users will benefit from these heightened protections even if their local laws have not been updated with more modern data privacy protections.

Companies and organizations that collect health information. Entities that elect to participate and adopt the framework will also benefit. First, they will stay ahead of the regulatory curve. By making pro-privacy decisions now, they will avoid having to make product changes that could be more expensive, time consuming, or complicated in response to future regulation.

Second, while entities will be able to develop and offer the product a consumer requests, they will be deterred from collecting and using health data they do not actually need. This should reduce both legal and reputational risks in a world where the public and enforcement agencies expect more from companies that handle data.

Finally, this model has the potential to provide some compliance certainty for members. By adopting more forward-looking privacy practices, companies and organizations will avoid practices in the gray or evolving areas of existing laws. Compliance with these standards would provide some assurance that participants have met various federal and state requirements.

Regulators and oversight bodies. Congress, the Federal Trade Commission, and their state-level counterparts will benefit from the commitment to publicly-available rules. It will allow them to enforce these promises, which will be more explicit than many existing privacy policies. Instead of engaging in complicated investigations and balancing tests, these entities will be able to measure compliance more easily.

Additionally, if the self-regulatory model includes third party audits or enforcement, there will be instances to investigate and prosecute, allowing these agencies to focus their resources on bad actors who would not otherwise be compelled to act in pro-privacy ways.

Attachment #2

Proposed Substance of Framework and Policy Rationale

For any follow up questions, kindly contact Andy Crawford at CDT (acrawford@cdt.org)

Definitions

1. **Affirmative Express Consent** -
    a. In General - The term “affirmative express consent” means an affirmative act by a consumer that clearly communicates the consumer’s authorization for an act or practice, in response to a specific request that -
        i. Is provided to the consumer in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms; and
        ii. Includes a description of each act or practice for which the consumer’s consent is sought and;
            1. Is written concisely and in easy-to-understand language; and
            2. Includes a prominent heading that would enable a reasonable consumer to identify and understand the act or practice.
    b. Express Consent Required - Affirmative express consent shall not be inferred from the inaction of a consumer or the consumer’s continued use of a service or product.
    c. Voluntary - Affirmative express consent shall be freely given and nonconditioned.

The data covered by this framework is inherently sensitive and it is crucial that consent for its collection, use, and sharing be meaningful. It has been repeatedly documented that hiding terms in a privacy policy does not meet this standard. To that end, this definition requires the clear and thorough presentation of information to users and clarifies that consent cannot be inferred from consumer inaction. Moreover, consumer consent must be voluntary and cannot be conditioned. This approach is also consistent with the FTC’s approach, other frameworks, and bipartisan constructions of affirmative express consent introduced during the 116th Congress, including comprehensive privacy legislation and legislation targeting consumer health information.

2. **Aggregated Data** - The term “aggregated data” means consumer health information that relates to a group or category of consumers but cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household. A participating entity wishing to use aggregated consumer health information shall -
    a. Take reasonable measures to safeguard the aggregated consumer health information from reidentification;
    b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the aggregated consumer health information with any consumer or device linked or reasonably linkable to a consumer;

c. Collect, disclose, or use the aggregated consumer health information for research purposes only; and

d. Contractually require the same commitment for all transfers of the aggregated consumer health information.

This framework recognizes that properly aggregated data should pose fewer privacy risks to individuals and communities. As a result of that reduced privacy risk, this framework permits certain uses of aggregated data because it can achieve positive societal purposes with fewer individualized risks, in ways that identifiable data sets cannot. Importantly, aggregation is not a silver bullet in protecting individual privacy. This framework includes requirements to limit the use of aggregated data to research purposes.

3. **Consumer** - The term "consumer" means an individual.

4. **Consumer Health Information** - The term "consumer health information" means -
    a. Any information, recorded in any form or medium, that—
        i. Is created or received by an entity; and
            1. Relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual; or
            2. Relates to the provision of health care to an individual, and
    b. The following data sets regardless of the purpose or outcome of the collection, disclosure, or use—
        i. Data that reflects racial and ethnic origin;
        ii. Genetic data;
        iii. Biometric data;
        iv. Data that reflects reproductive health;
        v. Data that reflects sexual orientation;
        vi. Data that reflects disability;[1]
        vii. Data that reflects sensitive disease conditions; and
        viii. Data that reflects substance abuse.

This definition intentionally rejects previous notions of "health data" that are limited to the direct provision of health services by a professional. It also avoids the approach taken by some other voluntary frameworks that create a list of health conditions that qualify for protection. This definition instead focuses on the nature of the information and how it is used. It recognizes that all data can be "health data" if it is used for those purposes, even if it appears unrelated on its face. To that end, subsection (a) covers all data that a participant collects, shares, or uses for health purposes. Subsection (b) declares that certain sensitive health topics shall always be subject to the framework, regardless of the context of their use. This framework does not include an exception for employee data.

[1] As defined under that Americans with Disabilities Act of 1990.

A purpose- and use-based approach to this definition has several benefits. First, it benefits consumers by raising the bar for all the data that is used to impact their health and wellness. Modern data use is complex, opaque, and instantaneous. Trying to delineate distinct data sets as worthy of coverage and others as not no longer makes sense for the people whose information is implicated. Second, it creates a tech-neutral standard that will stay relevant as technology evolves.

5. **Participating Entity** - The term "participating entity" means an entity or person that collects, gathers, or uses consumer health information in any form or medium for non-personal purposes and that adopts this framework.

This has been drafted broadly in an effort to capture all entities that collect and/or use consumer health information. It no longer makes sense for consumers to have different rights depending on what entities hold their information.

6. **De-identified Data** - The term "de-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that an entity in possession of consumer health information—
    a. Takes reasonable measures to ensure that the consumer health information cannot be reidentified, or associated with, an individual, a household, or a device used by an individual or household;
    b. Publicly commits in a conspicuous manner—
        i. To process and transfer the consumer health information in a de-identified form; and
        ii. Not to attempt to reidentify or associate the consumer health information with any individual, household, or device used by an individual or household; and
    c. Contractually obligates any person or entity that receives the information from the participating entity to comply with all of the provisions of this paragraph.

Similar to "Aggregated Data," it is critical to clearly define de-identified data within the framework. Properly de-identified data should pose fewer privacy risks to individuals and communities. To ensure that consumer privacy is protected, Section V below makes it clear that any participating entity seeking to utilize de-identified consumer health information must determine that the data is not individually identifiable by applying accepted methods and security practices. These reduced privacy risks allow de-identified data to be used in ways other identifiable data sets cannot under this framework.

7. **Publicly Available Information** - The term "publicly available information" means any information that -
    a. Has been lawfully made available to the general public from Federal, State, or local government records;
    b. Is published in a telephone book or online directory that is widely available to the general public on an unrestricted basis;

   c. Is video, audio, or internet content published in compliance with the host site's terms of use and available to the general public on an unrestricted basis; or
   d. A news media organization publishes to the general public on an unrestricted basis.

For the purposes of this definition, information is not restricted solely because there is a log-in requirement associated with accessing the information, or a fee of no more than $20 per month or per transaction. When a user of a social media service creates or shares information on that service, such information is restricted unless it is freely accessible by all users of the service.

Like many proposals, this framework recognizes that there is individual and societal value in the free flow of information and that even health data that has legitimately been made public may receive reduced protections. We have tried to craft this definition to capture truly public information while not being overly broad. We also clarify that traditional sources of news, like newspapers, whose digital presence may have a log-in and/or small cost associated with their service, is still considered well within the public sphere.

8. **Privacy Review Board** - The term "privacy review board" means an independent board that -
   a. Is comprised of at least three members;
   b. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
   c. Includes at least two members who are not affiliated with the participating entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities;
   d. Includes at least one member who is a consumer representative; and
   e. Does not have any member participating in a review of any project in which the member has a conflict of interest.

Review boards inject valuable, independent professional review for certain proposed uses of consumer health data. Large and consequential uses of consumer health information will benefit from this independent scrutiny. In an effort to stay consistent and not introduce a host of new terms or requirements, this definition is heavily influenced by similar provisions within HIPAA and its accompanying regulations.

9. **Research** - The term "research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

This definition is heavily influenced by similar provisions within HIPAA, the Common Rule regarding federal human subjects, and their respective regulations. This definition permits *public interest research to continue while avoiding a loophole that could be used to justify and type of commercial data research.*

Collection and Processing of Consumer Health Information

I. Transparency and Notice

Transparency and notice serve two functions. First, both allow individual consumers to make informed decisions before they agree to have their health information collected, disclosed, or used. Second, transparency and notice requirements allow researchers, regulators, and advocates to track data use trends and better understand companies' practices. Because these purposes require a different level of detail, the framework requires two sets of notice. This approach provides consumers with the information they need without overwhelming them, while simultaneously providing more thorough information to be used in the public interest.

Elements of Notice:

A participating entity shall not collect, disclose, or use consumer health information unless it provides the following information to consumers before any data is collected, disclosed, or used—

1. Clearly identifies the types of health information that will be collected.
2. Clearly states the purpose(s) that any health information is collected for.
3. States if any health information will be disclosed, and if so, provides the user with the names of all the entities that will receive, license, or purchase the consumer health information.
4. States the reasons that any health information is disclosed.
5. Notifies consumers when policies and practices surrounding how their health information will be collected, disclosed, or used have changed.
6. Provides consumers with a description of the consumer's individual rights and a clear list of any consumer controls that a participating entity has made available.

Forms of Notice:

A participating entity that collects, discloses, or uses consumer health information shall, with respect to each service or product provided by the participating entity, publicly publish—

1. A consumer-facing policy that—
   a. Includes information regarding each element listed within the "elements of notice" section of this framework; and
   b. Must be written in a manner that is succinct and easily understandable to a consumer.

2. A complete second and more detailed policy that includes—
   a. The specific types of consumer health information collected;

  b. The manner in which consumer health information is collected;
  c. The purposes for the consumer health information collection;
  d. The security and retention procedures for how the participating entity handles consumer health information; and
  e. A detailed list of all third parties with whom the participating entity has disclosed or plans to disclose consumer health information.

Section 1 is designed to inform consumers as they engage with a participant's product. Section 2 is designed to provide more information for civil society groups, researchers, reporters, and regulators that wish to conduct oversight of the collection and use of consumer health information.

II. Consent

Elements of Consent:

Before a participating entity may collect or use consumer health information—

1. A participating entity must obtain affirmative express consent from a consumer that details the purpose and intended use from the individuals whose health information will be collected, disclosed, or used.
2. Affirmative express consent shall be freely given and nonconditioned.

A participating entity collecting, disclosing, or using consumer health information must limit the collection, disclosure, or use of consumer health information to only what the consumer has expressly consented to.

1. A participating entity must seek additional consent for any new collection, disclosure, or use of consumer health information outside the scope of any previous consumer consent.
2. A participating entity collecting, disclosing, or using consumer health information must provide consumers with the ability to revoke consent.
    a. A participating entity must stop the collection, disclosure, or use of health information once a consumer has revoked consent.

These provisions are drafted to require consumer consent around specific collections and uses of consumer health information as opposed to a simple blanket consent for a host of possible uses. It also includes important consumer rights to revoke consent later on.

III. Consumer Controls

Consumer Rights with Respect to Consumer Health Information:

1. Consumers' Right to Access, Correct, and Delete Consumer Health Information

   a. A participating entity shall provide a consumer with a free, clear, and easy process for requesting personal consumer health information within the participating entity's possession.
   b. A participating entity shall provide a consumer with a free, clear, and easy process for requesting corrections or deletions to any inaccurate information within the consumer health information within the participating entity's possession.
   c. A participating entity shall make reasonable efforts to correct or delete a consumer's health information based upon a consumer's request for correction or deletion.
      i. When correction or deletion cannot occur, a participating entity shall provide the requesting consumer with an explanation as to why the correction or deletion request cannot be carried out.

2. Consumers' Portability Rights
   a. Where technically feasible, a participating entity shall make available a reasonable means for a consumer to transmit or transfer their health information that is retained by the participating entity to another participating entity in a structured, standardized, and machine-readable interoperable format, or otherwise download personal information for the consumer's own use.

3. The Use of Consumer Health Information to Train or be the Subject of Automated Systems or Processes
   a. A participating entity shall not collect, disclose, or use consumer health information to train or be the subject of any automated, algorithmic, or artificial intelligence application unless that entity has first:
      i. Obtained affirmative express consent from a consumer for the use of their health information in such applications, or
      ii. Subjected the consumer health information to be collected, disclosed, or used to a risk-based privacy assessment and any risks identified have been appropriately mitigated, and the use is consistent with a reasonable individual's expectations given the context in which the individual provided or authorized the collection, disclosure, or use of their consumer health information.
   b. Automated, algorithmic, or artificial intelligence applications, processes, and systems must be designed and implemented by the participating entity to mitigate potential algorithmic bias, including through design processes that regularly interrogate the variables and training data used, measures that ensure transparency and explainability, and routine auditing.

We have drafted this section to include several consumer rights that are consistent with existing domestic and international regulations and proposals.

IV. Obligations for Participating Entities

Attachment #2

Currently, the burden of ensuring sufficient privacy protections around health data disproportionately falls on consumers. This portion of the framework focuses on data collection and use practices that ensure data is used for limited purposes consistent with consumer requests and expectations. We have also included data security provisions.

Relation to Existing Federal, State, and Municipal Laws and Regulations:

To the extent that any participating entity's collection, disclosure, or use of consumer health information is already governed by Federal, State, and Municipal laws or regulations, those legal obligations are not affected by this framework.

This section is intended to make clear that framework participants must follow all applicable laws and regulations in addition to offering consumers the higher level of protections included within the framework.

Permissible Collection and Use Practices for Consumer Health Information:

1. A participating entity—
    a. Shall not collect, disclose, or use consumer health information for any purpose other than what the data was originally collected, disclosed, or used for;
    b. Shall limit the amount of consumer health information collected, disclosed, or used to only what is necessary to provide the product or feature the consumer has requested,
    c. Shall take reasonable efforts to ensure the third parties and service providers with whom it shares consumer health information meet the obligations of this framework.

This section is intended to categorically prohibit secondary uses of health data that do not fall under one of the clearly defined exceptions to this framework. If a participating entity would like to offer a new product, functionality, or repurpose data for any reason, they must start the notice and affirmative consent process over. In no instance should terms of service serve as justification for secondary uses of data. Data collection and use limits carry through to third parties. Consumers should be protected without having to take additional steps to monitor how their data is being used by third parties.

This section is likely to curb some current behavioral advertising and commercial product development activities that do not avail themselves of one of the other exceptions like the use of de-identified data. We understand this approach is more stringent than other voluntary frameworks or legal standards, but believe health data warrants the protection.

Consumer Health Information Retention:

1. A participating entity -

   a. Shall maintain consumer health information for a period of time only as long as necessary to carry out the purpose(s) for which the consumer health information was collected;
   b. Shall delete all consumer health information once there is no longer a valid reason to retain it.

There should be clear and reasonable limits on the length of time consumer health information may be maintained by participating entities. Retention limits benefit both consumers and participants. Less data can lessen the impact of breaches and ensure that decisions are not made on stale, old, and incorrect data, and produces lower storage and security costs. These limits are consistent with limits in other existing proposals and regulations.

Prohibitions on the Use of Consumer Health Information to Harm or Discriminate Against Consumers:

1. A participating entity shall not collect, disclose, or use consumer health information when making eligibility determinations around housing, employment, healthcare, and other critical determinations.
2. A participating entity must ensure equal access and accommodation considerations when collecting, disclosing, or using consumer health information.

Consumer health information is inherently sensitive. It should not be collected, disclosed, or used in ways that harm, discriminate against, or limit consumer's access to critical life opportunities.

Security:

1. A participating entity shall establish and implement reasonable information security policies, practices, and procedures for the protection of consumer health information, taking into consideration—
   a. The nature, scope, and complexity of the activities engaged in by such participating entity;
   b. The sensitivity of any consumer health information at issue;
   c. The current state of the art in administrative, technical, and physical safeguards for protecting such information; and
   d. The cost of implementing such administrative, technical, and physical safeguards.
2. Requirements - The policies, practices, and procedures required in subpart (1) of this section must include the following:
   a. A written security policy with respect to the processing of such consumer health information.
   b. The identification of an officer or other individual as the point of contact with responsibility for the management of information security.
   c. A process for identifying and assessing reasonably foreseeable security vulnerabilities in any systems maintained by such participating entities that

contain such consumer health information, which shall include regular monitoring for vulnerabilities and breaches of security of such systems.

d. A process for taking action designed to mitigate against vulnerabilities identified in the process required by subparagraph (c)—which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software—or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards.
e. A process for determining if consumer health information is no longer needed and disposing of consumer health information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such consumer health information permanently unreadable or indecipherable.
f. A process for overseeing persons who have access to consumer health information, including through network-connected devices.
g. A process for employee training and supervision for implementation of the policies, practices, and procedures required by this subsection.
h. A written plan or protocol for internal and public response in the event of a breach of security.

This section imposes a “reasonable” security requirement on participants which is consistent with FTC enforcement and the laws in many states. Because “reasonable” is scaled to the sensitivity of the data, the way it is used, and the state of technology, participants’ obligations will be commensurate with the business and engineering decisions they make. The processes required here are also flexible and outcome based which is usable for participants of all sizes and sophistication.

V. Exceptions

Nothing in this framework shall limit participating entities from:

1. Engaging in practices that utilize consumer health information when necessary and solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes that adhere to commonly accepted ethical standards and laws,
   a. With affirmative express consent from a consumer; or
   b. For research that has been reviewed and approved by a privacy review board; or
   c. For research utilizing de-identified consumer health information, provided that—
      i. A participating entity may utilize de-identified consumer health information for research in the public interest without consumer consent only after it determines that consumer health information is not individually identifiable. This determination shall be made by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, who:

            1. Applying such principles and methods, determines that the risk is very small that the consumer health information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
            2. Documents the methods and results of the analysis that justify such determination.

    d. For research utilizing aggregated consumer health information, provided that—

        i. A participating entity may utilize aggregated consumer health information for research in the public interest without consumer consent only after it—

            1. Determines that the consumer health information to be used only relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual, and
            2. Documents the methods and results of the analysis that justify such determination.

2. Engaging in commercial, academic, or research practices that utilize publicly available consumer health information so long as—
    a. A participating entity does not collect, disclose, or use publicly available consumer health information when making eligibility determinations around housing, employment, and other critical determinations; and
    b. A participating entity ensures equal access and accommodation considerations when collecting, disclosing, or using publicly available consumer health information.
3. Using or disclosing consumer health information to a medical professional or health care provider without consumer consent if that participating entity, in good faith—
    a. Believes that an emergency involving danger of death or serious physical injury to any person requires use or disclosure relating to the emergency, and
    b. Believes that any recipient of this information is in a position to address, rectify, or prevent the emergency.
4. Engaging in practices that utilize consumer health information when necessary and solely for purposes of—
    a. Detecting and preventing security incidents, identity theft, or fraud or protecting against malicious or deceptive activity;
    b. Identifying or repairing errors that impair existing intended functionality;
    c. Complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process.
    d. Addressing health misinformation or moderating content or accounts to prevent harm to consumers.

The framework should include very limited exceptions that permit the collection, use, and sharing of health data without consent or for secondary purposes. Mindful of how exceptions *can undercut the effectiveness of a framework, these provisions borrow from long-standing laws that attempt to balance the equities between individual privacy, societal benefits from the use of this data, and participant needs to process data to deliver the service or product requested by an individual.*

Attachment #2

Proposed Framework Structure: Self-Regulatory Program

For any follow up questions, kindly contact Alice Leiter at eHI (alice@ehi.org)

The proposed program is one of accountability: a self-certification program designed to hold member companies to a set of standards separately developed through a multi-stakeholder process. The program would accept individual companies as members.[2] These members would undergo a thorough onboarding review at enrollment, be educated as to the self-regulatory framework, publicly commit to complying with it, and submit to annual assessments. Additionally, active "spot-check" monitoring would be done on a random sample of members throughout each year. Companies would hold themselves out to the public as a "XXX Health Data Participant" (name TBD).

User fees would be collected to maintain this program, and the amount of the fee would be on a sliding scale – likely based on the size of the company in terms of gross sales.

Relevant components/details of this program would include:

- Robust standards governing the program's onboarding reviews, annual compliance assessments, and ongoing monitoring of participant companies;
- Criteria to ensure that the reviews and assessment conducted by the program are independent of program's administrative and financial functions;
- A public commitment by each company to follow the program's standards;
- Maintenance by the program of a dedicated, public-facing website describing the program's goals and requirements, listing participating covered organizations, and providing an effective method for consumers to ask questions and file complaints about any program and/or any participating covered organization;
- A standardized set of privacy rules, that include:
    - A broad, use-based, definition of consumer health information;
    - Clear notice requirements;
    - Greater consumer access and control of their health information; and
    - Articulated appropriate uses and obligations surrounding the collection and use of consumer health information.
- An annual report by the program to the public detailing the program's activities and effectiveness during the preceding year in obtaining compliance by participating covered organizations and in taking meaningful disciplinary action for non-compliance.

[2] Included entities will be any company that collects, uses, or processes health-related personal data. These would include: hardware manufacturers; App developers; website publishers third-party data management, brokering, collection, or use outfits; potentially businesses/employers that rely on third-party health technology in order to maintain health of their workers.

Enforcement could include:

- Independent monitoring by program staff or other authorized evaluators, including publicly announced cases;
- Active complaint-gathering process;
- Requirement to develop a corrective action plan (CAP);
- Process to lose certification if CAP fails
- Penalties for persistent or willful non-compliance with the law and the program's standards, such as suspension or dismissal from the program, and/or referral to the FTC and/or state AG;
- Potential for FTC and/or state AG enforcement of violation of agreed to industry agreement; and
- A dispute resolution mechanism for resolving consumer complaints or complaints by another company based on the program's standards about non-HIPAA health data and potentially providing consumers with redress for violations.

This type of self-certification program would help to level the playing field among businesses, fostering a unified set of privacy practices that are responsive to recent regulation (the standards would presumably ensure compliance with the most stringent and/or far-reaching state laws), while raising the bar for consumer privacy in an area of great personal sensitivity. The critical difference between this program and a more passive pledge-style or "best practices" program is the inclusion of rigorous onboarding and ongoing accountability assessments, all of which are designed to elicit full compliance from well-intentioned actors and prevent bad actors from falsely shielding their inappropriate conduct behind a pledge Significantly, such a program could be easily converted into a safe harbor-style accountability mechanism in future legislation, giving it lasting utility even should new laws come about.

We aim to incorporate as much consumer input as possible in the establishment and operationalization of this program, with emphasis on its functioning as a bridge to legislation, rather than a final solution to the issue of under-protected data. In order for this program to be successful, it will need widespread consumer buy-in and trust, and the best way to achieve this is to involve consumers and consumer advocates in the design of the program itself.

Finally, although this program would depend on participation fees for its ongoing operations, it would require seed capital to establish initial operations. Given this, combined with a significant number of outstanding logistical issues, we see significant value in housing this program in an existing organization with established infrastructure and experience running self-regulatory programs, such as BBB National Programs.

Attachment #2

How to Submit Feedback

We are looking for feedback on all aspects of the *Draft Framework*. Comments will be accepted until **Friday, September 25, 2020.**

To submit comments, please mail Alice Leiter at eHI (alice@ehidc.org) or Andy Crawford at CDT (acrawford@cdt.org), or visit https://www.ehidc.org/resources/draft-consumer-privacy-framework-health-data.

Attachment #3

CONFIDENTIALITY
COALITION

***Submitted electronically via* https://www.ehidc.org/resources/draft-consumer-privacy-framework-health-data**

September __, 2020

Alice Leiter
Vice President and Senior Counsel
eHealth Initiative and Foundation
Alice@ehidc.org

Andy Crawford
Policy Counsel
Center for Democracy & Technology Data and Privacy Project
acrawford@cdt.org

Re: Draft Consumer Privacy Framework for Health Data Comments

Dear Ms. Leiter and Mr. Crawford:

The Confidentiality Coalition appreciates the opportunity to submit comments on the "Proposed Consumer Privacy Framework for Health Data" by the eHealth Initiative (eHI) and Center for Democracy & Technology (CDT) that was released for public comment on August 27, 2020 (Draft Framework).

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective confidentiality protections for health care consumers. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and health care consumers while, at the same time, enabling the essential flow of information that is critical to the timely and effective delivery of health care, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

General Comments
Before commenting on specific sections of the Draft Framework, the Confidentiality Coalition would like to commend eHI and CDT for creating this proposal to address the

gaps in the legal protections for health data outside HIPAA's protections. We share the same concerns as eHI and CDT regarding the unregulated nature of this data and would like to underscore the need for a framework, ultimately regulatory in nature, to protect health records in the hands of non-HIPAA entities. As indicated in the Background section [but which could be stated with greater specificity], this need has become more urgent since the issuance in May 2020 of the ONC 21st Century Cures Act final rule by the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology and the Interoperability and Patient Access final rule by the Centers for Medicare and Medicaid Services. These rules will facilitate and accelerate the transfer of protected health information from HIPAA entities to non-HIPAA entities, such as third-party apps. While the intent is to give consumers greater control over their own health data, it will also result in many more health records falling outside of the strong protections of HIPAA, oftentimes without consumers understanding this or appreciating its implications.

The Confidentiality Coalition has long sought to advance a framework to protect personal health information that is not already covered by HIPAA. To this end, it has developed a set of privacy principles, "Beyond HIPAA Privacy Principles" (a copy of which is attached to these comments) that outline our views on the protection of this health data. As stated in these principles, the Confidentiality Coalition believes that health data falling outside HIPAA should be subject to uniform, national privacy and security rules comparable to HIPAA. To foster and retain consumer trust, the framework for these standards should ultimately be established through legislation enacted by Congress, with meaningful penalties and enforcement by a federal regulatory agency. However, until then, we support a voluntary framework that provides strong protections and harmonizes with HIPAA so as to facilitate compliance and the appropriate flow of health information.

Specific Comments

Below are our comments on some of the specific concepts and provisions in the Draft Framework.

1. Definitions

The Draft Framework defines and distinguishes between "consumer health information" (CHI), "aggregated data" and "de-identified data", noting that the latter two types of data pose fewer privacy risks. We support this distinction, and believe that it is important for participating entities to be encouraged to use aggregated or de-identified data wherever possible instead of CHI.

To ensure that this occurs, the definition of CHI should make clear that it is limited to information that can reasonably be linked to a unique individual or household. Device data should be included only to the extent that the device can in turn be linked to a unique individual or household. As currently written, paragraph a. of the definition of CHI requires that the information "relate" to an individual, but not necessarily an identified or reasonably identifiable individual. Similarly, the data sets listed in paragraph b. of the definition are not necessarily limited to data about an identified or reasonably identifiable individual. The definition of CHI should also clearly exclude aggregated data, de-identified data and publicly available information. To avoid confusion on this point, the Draft Framework should not refer to "aggregated consumer health information," "de-identified consumer health information" or "publicly available consumer health information." Similarly, the definitions of "aggregated data, "de-identified data" and "publicly available information" should each make clear that they are a not subsets of CHI and, in the case of de-identified data, that it cannot reasonably be linked to an "identified or identifiable" individual.

We also strongly encourage eHI and CDT to look to the HIPAA definition of de-identified data as the basis for the definition in the Draft Framework. The HIPAA definition provides two distinct methods or pathways for de-identifying protected health information, namely, the safe harbor method and the statistical expert method. Both methods are well established and well understood and provide specific standards that can be used by HIPAA entities to render information de-identified. As currently written, the Draft Framework appears to require a method of de-identification similar to the HIPAA expert method, at least with respect to uses for research purposes, but does not provide for a simpler method, similar to the safe harbor method, that would not require the use of a statistical expert. Providing similar de-identifications standards to those in HIPAA, and regardless of the purpose for which the de-identified data is used, would allow participating entities to draw on the experience gained in HIPAA. It would also provide consumers with the assurance that consistent and robust standards for de-identification are applied before broader use of the data is permitted. While there is no definition of "aggregated data" in HIPAA, it would be similarly helpful to provide clear standards or criteria for data to qualify as aggregated, and through a simpler methodology than statistical analysis. It would also be helpful if the definition made clear whether aggregated data is intended to be distinguishable from aggregated de-identified data and, if so, how.

Finally, consistent with the Background and Project Goals and Status sections, which make clear that the intent of the Draft Framework is to address health data "outside HIPAA's coverage," the definition of CHI should explicitly exclude protected health information governed by HIPAA.

2. Use of Aggregated and De-identified Data

The Confidentiality Coalition is mindful that aggregating or de-identifying data is not a "silver bullet" in that there still remains a risk of re-identification, however small. However, consistent with the goal of encouraging the use of aggregated and de-identified data instead of identifiable data wherever possible, we recommend that the Draft Framework ["allow broader use of these data sets" OR "allow such data to fall outside the framework in the same way as de-identified data falls outside of HIPAA"]. As written, it appears that aggregated data may be used only for research purposes, and that participating entities could not even request consumers to consent to the use of such data more broadly. This would exclude the use of such data for many beneficial purposes such as training, quality assurance, population health, safety evaluations, products or service improvement, to name only a few.

While the definition of de-identified data does not limit its use for research purposes, and the comment in the section on “Permissible Collection and Use Practices” suggests that de-identified data could be used for “current behavioral advertising and commercial product development activities”, there is no exception in Section V for this purpose. There is also no general exception for use of de-identified data. Such an exception and the exclusion of de-identified data from CHI would make clear to participating entities that they may use such data for any lawful purpose.

3. Use of Publicly Available Information

The Confidentiality Coalition agrees that there is individual and societal value to the free flow of information that has legitimately been made public. Therefore, while we agree that publicly available information should not be permitted to be used for discriminatory purposes as appears to be the intent of the exception Section V.1.d, we are concerned that the Exception may be read to limit publicly available information to only the purposes specified in the exception. For example, publicly available information on physicians and other health care professionals is currently used for valuable public policy purposes, including quality improvement and evaluation, and these types of uses should continue to be permitted. While we do not believe the definition of CHI is intended to encompass this type of data or that the Draft Framework is intended to limit the use of such data for lawful purposes, we recommend that the Draft Framework make clear that publicly available information falls outside its ambit to avoid confusion or have a chilling effect on the many beneficial uses of publicly available information.

4. Transparency and Notice

We agree that transparency and notice to consumers are essential in order for consumers to be able to make informed decisions regarding the disclosure of their health information. A clear and simple description of an entity’s data collection practices and a consumer’s data rights is also critical in order to be able to move away from reliance on a consent-based model. We particularly support the concept of a layered or two-tier notice for consumers. This would allow a consumer to learn, through a succinct and consumer-friendly cover or first notice, of their data rights and the key privacy practices of a participating entity, with a second more detailed notice being available to provide additional information on the entity’s privacy practices, and information on how consumers may exercise their data rights.

However, we are concerned that requiring a listing by name of every entity with which the participating entity has or will share CHI is not practicable or even helpful to consumers. In addition, there are many different reasons -- some in the public interest, but others potentially not -- that other entities, including competitors, may be interested in this type of information, and it is not clear that these entities, other than regulators, should have an automatic right to know this level of detail. The Draft Framework could potentially include a consumer right to request certain information about non-routine disclosures that the participating entity makes of CHI generally. This would strike a reasonable balance between the consumer’s interest and the administrative burden on the participating entity, since experience with the HIPAA right to an accounting, which imposes a significant burden on HIPAA entities, has shown that most consumers do not have an interest in, or benefit from, knowing detailed information about each non-routine disclosure of their information.

5. Consent

The Confidentiality Coalition strongly supports the goal of moving "beyond outdated notice and consent models" so as to "shift the burden of privacy risk off consumers." Such an approach is consistent with the approach in HIPAA, which allows use of protected health information for treatment, payment and health care operations after the provision of the covered entity's notice of privacy practices but without requiring an individual's affirmative consent or authorization. Similarly, in the Draft Framework, participating entities should be required to provide a clear and concise notice of their data collection practices to consumers and then be permitted to use a consumer's CHI for the purposes for which it was provided by the consumer (i.e., consistent with the consumer's reasonable expectations in the circumstances) without having to obtain the consumer's affirmative express consent. Any other use outside of the original purpose and expectations should require the consumer's affirmative express consent, subject to limited exceptions for public policy purposes similar to those allowed in HIPAA. In addition, when CHI is shared for a public policy purpose, the recipient of the CHI should be limited to using and disclosing the data only for the public policy purpose for which it was provided to the entity. We share the concern about blanket consents that would allow use of CHI "for a host of possible uses," and therefore, agree that any affirmative express consent should be specific and narrowly construed.

However, we do not believe that obtaining written consent for uses that are consistent with a consumer's request or reasonable expectations is beneficial or meaningful. This would simply perpetuate the outdated consent model where consumers are required in a rote fashion to check boxes or sign forms before being able to proceed. This approach imposes administrative burdens and operational hurdles without any commensurate consumer benefit and, indeed, would create the illusion of consumer control. As in the HIPAA framework, consumers that choose to request or use certain products or services that require use of their health data should reasonably expect that their health data will be used to support the provision of those products or services.

6. Service Providers

The Draft Framework states that participating entities must make "reasonable efforts to ensure" that third parties with whom they share CHI meet the obligations of this framework. The Confidentiality Coalition supports requiring service providers to be subject to the same obligations as the participating entity. Given the relationship, and similar to the HIPAA approach to business associates, we believe that the Draft Framework should affirmatively require that service providers be bound to the same obligations through a written agreement. In addition, participating entities should have responsibility for ensuring compliance with the Draft Framework by their service providers. This could include requiring an initial evaluation of the service provider's privacy and security capabilities, as well as ongoing monitoring of service providers through periodic audits or third-party assessments.

With respect to third parties that are not service providers, a “reasonable efforts” standard to obtain a similar contractual commitment to comply with the framework may be appropriate for some third parties that are not service providers, but not others. For example, in the case of disclosures to government agencies or in legal proceedings, it may not be feasible or appropriate to require the third party to agree to comply with the framework. In addition, while participating entities may ensure that third parties commit to complying with the framework, they will generally not be in a position to “ensure” such compliance with third parties that are not service providers.

7. Security

The Confidentiality Coalition supports the inclusion of security requirements in the Draft Framework. Even though the primary focus of the framework is on privacy protections, without reasonable security standards a privacy framework will have little value. We also strongly support the flexible, outcome-based scaled approach described in the Draft Framework, which appropriately takes into account the sensitivity of the data, the nature of its uses and the state of technology.

8. Proposed Structure of the Framework

The Confidentiality Coalition supports the program’s emphasis on robust initial vetting and ongoing accountability. We agree that this is critical to ensure that the program does not become a shield for bad actors or viewed as no more than a rubber stamp for dues-paying members. In light of this, we recommend that the Draft Framework provide at least a high-level description of the process and standards that will be involved in the initial onboarding and ongoing audits and assessments.

Finally, we believe a rigorous and independent onboarding and ongoing monitoring process is essential to engender the necessary consumer buy-in and trust. This trust, and the program’s viability as an interim substitute for legislation, will depend on the program’s certifying entity, as well as that of any program staff and auditing entities, being transparently independent. Therefore, greater clarity on the criteria and process to determine and maintain this independence would be helpful to build confidence in the Draft Framework.

The Coalition appreciates the opportunity to provide comments on the Draft Framework and stands ready to work with eHI and CDT as they seek to finalize it. Once implemented, we believe such a framework can provide meaningful protections for health data until such time as comprehensive national privacy legislation can be enacted. Please contact me at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

Attachment #4

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

Updated Guidance on HIPAA and Contacting Former COVID-19 Patients about Plasma Donation August 2020

Does the HIPAA Privacy Rule permit a covered health care provider or health plan to use protected health information (PHI) to identify and contact individuals who have recovered from COVID-19 to provide them with information about donating plasma that could be used to help patients with COVID-19?

Yes. Generally, a covered health care provider (*e.g.*, a hospital, pharmacy, or laboratory) or health plan may use PHI to identify individuals who have recovered from COVID-19 to provide them with information about how they can donate their plasma containing antibodies to SARS-CoV-2 (the virus that causes COVID-19) for use in potentially treating patients with COVID-19.[1]

The HIPAA Privacy Rule permits HIPAA-covered entities (or their business associates on the covered entities' behalf) to use or disclose PHI for treatment, payment, and health care operations, among other purposes, without an individual's authorization.[2] Health care operations include case management and care coordination activities that do not meet the definition of treatment (*e.g.*, where a health plan undertakes case management or care coordination, or where a health care provider undertakes such activities in a manner that is not connected to the care of a specific individual).[3] When using or disclosing PHI for health care operations, the covered entity must make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.[4]

[1] Plasma collected from individuals who have recovered from an infection is called "convalescent plasma." The Food and Drug Administration (FDA) has issued guidance to provide recommendations to health care providers and investigators on the administration and study of investigational convalescent plasma collected from individuals who have recovered from COVID-19 (COVID-19 convalescent plasma) during the public health emergency. *See* FDA, "Investigational COVID-19 Convalescent Plasma: *Guidance for Industry" (May 2020),* available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/investigational-covid-19-convalescent-plasma.

[2] *See* 45 CFR 164.502(a)(1)(ii) and 164.506.

[3] *See* 45 CFR 164.501 (defining "health care operations," and "treatment"). Additional discussion of the difference between treatment and health care operations under the HIPAA Privacy Rule can be found in the 2000 Final Privacy Rule, 65 FR 82462, 82626 (December 28, 2000).

[4] *See* 45 CFR 164.502(b) and 164.514(d).

The use of PHI to identify and contact individuals who have recovered from COVID-19 to inform them about how to donate plasma is permitted as a health care operations activity to the extent that facilitating the supply of donated plasma would be expected to improve the covered health care provider's or health plan's ability to conduct case management for patients or beneficiaries that have or may become infected with COVID-19.[5]

A covered health care provider or health plan may identify and contact individuals for this purpose, without authorization, to the extent that this activity does not constitute marketing. Marketing is a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service.[6] Generally, the HIPAA Privacy Rule prohibits the use or disclosure of PHI for marketing purposes without an individual's authorization.[7] Thus, communications that inform or encourage individuals who have recovered from COVID-19 regarding the means and benefits of donating plasma, and that encourage such individuals to use any particular blood or plasma donation center(s) for such donations, would constitute marketing, unless the communication meets an exception to the definition of marketing. Under one exception, a covered health care provider or health plan is permitted to make such communication for the covered entity's case management and related health care operations activities,[8] provided that the covered entity receives no direct or indirect payment from, or on behalf of, the third party whose service is being described in the communication (*e.g.,* a blood or plasma donation center).[9]

While the HIPAA Privacy Rule permits a covered entity to use PHI to identify and contact its own patients or beneficiaries who have recovered from COVID-19, a covered entity generally cannot disclose PHI to a third party, including another HIPAA-covered entity, without the individuals' authorization, for the third party to make marketing communications about the third party's products or services, unless the third party is making the communication on behalf of the covered entity (*i.e.,* as a business associate). For example, a covered health care provider or health plan cannot disclose PHI about individuals who have recovered from COVID-19 to a blood or plasma donation center, for the donation center's own purposes.[10] In such cases, the covered health care provider or health plan would need to obtain the individuals' authorization prior to making such a disclosure.

[5] *See* 45 CFR 164.501 (definition of "health care operations" (1): "Conducting . . . case management and care coordination . . . and related functions that do not include treatment . . . .").

[6] *Se*e 45 CFR 164.501 (definition of "marketing," ¶ 1).

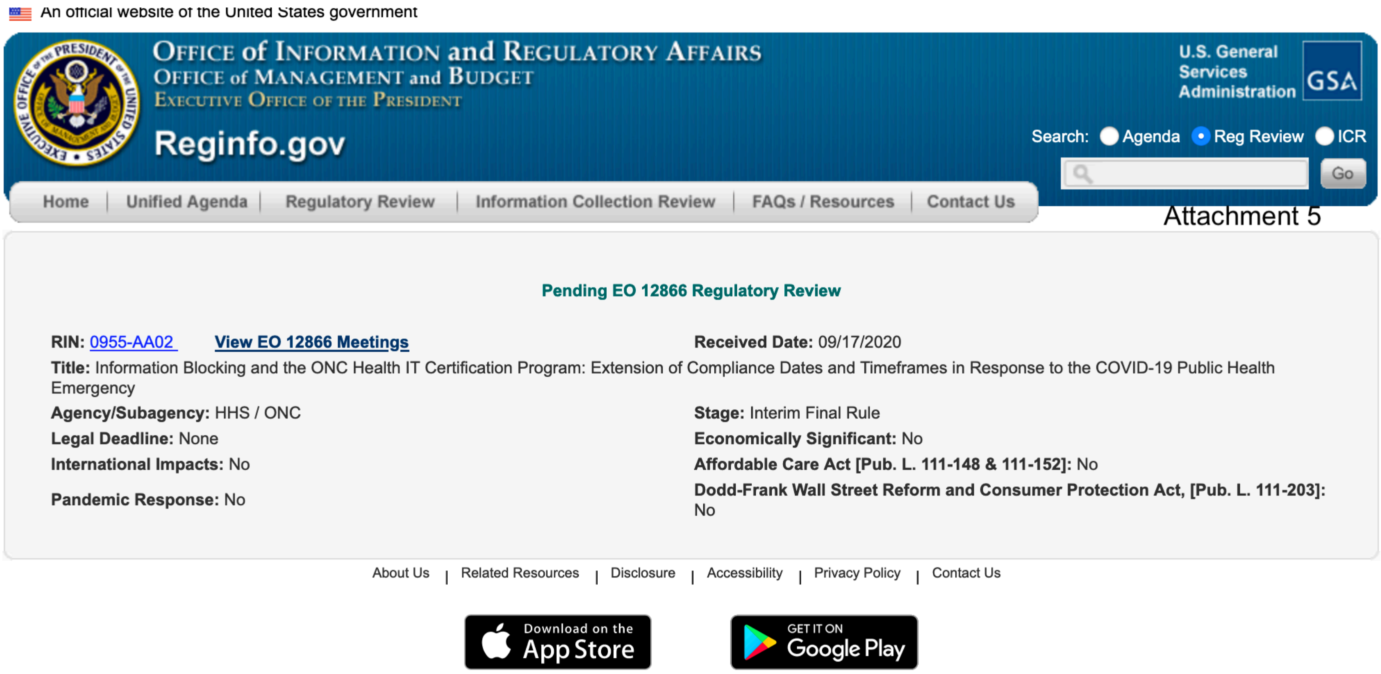
[7] *Id.*

[8] *See* 45 CFR 164.501 (definition of "marketing," ¶ (2)(ii)(C)).

[9] *Se*e 45 CFR 164.501 (definition of "marketing," ¶¶ (2)(ii)(C), (3)).

[10] A disclosure to the blood or plasma donation center, for the blood or plasma donation center's own purposes, is not considered to be made for the health care operations of the covered health care provider or health plan. However, a covered health care provider or health plan may disclose PHI about individuals who have recovered from COVID-19 to a blood or plasma donation center that is working with the provider or plan to improve the provider's or plan's ability to conduct case management for individual patients or beneficiaries, or for patient or beneficiary populations, that have or may become infected with COVID-19, if the covered provider or plan enters into a business associate agreement with the blood or plasma donation center.

Attachment 5


An official website of the United States government
Office of Information and Regulatory Affairs
Office of Management and Budget
Executive Office of the President
Reginfo.gov
U.S. General Services Administration
GSA
Search: ○ Agenda ● Reg Review ○ ICR
Go
Home
Unified Agenda
Regulatory Review
Information Collection Review
FAQs / Resources
Contact Us

Pending EO 12866 Regulatory Review

RIN: 0955-AA02 **View EO 12866 Meetings** **Received Date:** 09/17/2020

Title: Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency

Agency/Subagency: HHS / ONC	**Stage:** Interim Final Rule
Legal Deadline: None	**Economically Significant:** No
International Impacts: No	**Affordable Care Act [Pub. L. 111-148 & 111-152]:** No
Pandemic Response: No	**Dodd-Frank Wall Street Reform and Consumer Protection Act, [Pub. L. 111-203]:** No

About Us | Related Resources | Disclosure | Accessibility | Privacy Policy | Contact Us
Download on the App Store
GET IT ON Google Play

Attachment #6

116TH CONGRESS
1ST SESSION

S. ______

To establish data privacy and data security protections for consumers in the United States.

IN THE SENATE OF THE UNITED STATES

Mr. WICKER (for himself, Mr. THUNE, Mrs. BLACKBURN, and Mrs. FISCHER) introduced the following bill; which was read twice and referred to the Committee on ____________________

A BILL

To establish data privacy and data security protections for consumers in the United States.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or the "SAFE DATA Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Attachment #6

TITLE I—INDIVIDUAL CONSUMER DATA RIGHTS

TITLE II—DATA TRANSPARENCY, INTEGRITY, AND SECURITY

TITLE III—CORPORATE ACCOUNTABILITY

TITLE IV—ENFORCEMENT AUTHORITY AND NEW PROGRAMS

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—The term ‘‘affirmative express consent’’ means, upon being presented with a clear and conspicuous description of an act or practice for which consent is sought, an affirmative act by the individual clearly

communicating the individual's authorization for the act or practice.

(2) ALGORITHM.—The term "algorithm" means a computational process derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that processes covered data for the purpose of making a decision or facilitating human decision-making.

(3) ALGORITHMIC RANKING SYSTEM.—The term "algorithmic ranking system" means a computational process, including one derived from algorithmic decision-making, machine learning, statistical analysis, or other data processing or artificial intelligence techniques, used to determine the order or manner that a set of information is provided to a user on a covered internet platform, including the ranking of search results, the provision of content recommendations, the display of social media posts, or any other method of automated content selection.

(4) BEHAVIORAL OR PSYCHOLOGICAL EXPERIMENTS OR RESEARCH.—The term "behavioral or psychological experiments or research" means the study, including through human experimentation, of overt or observable actions and mental phenomena inferred from behavior, including interactions be-

Attachment #6

tween and among individuals and the activities of social groups.

(5) COLLECTION.—The term ''collection'' means buying, renting, gathering, obtaining, receiving, or accessing any covered data of an individual by any means.

(6) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(7) COMMON BRANDING.—The term ''common branding'' means a shared name, servicemark, or trademark.

(8) COMPULSIVE USAGE.—The term ''compulsive usage'' means any response stimulated by external factors that causes an individual to engage in repetitive, purposeful, and intentional behavior causing psychological distress, loss of control, anxiety, depression, or harmful stress responses.

(9) CONNECTED DEVICE.—For purposes of paragraphs (20) and (37), the term ''connected device'' means a physical object that—

(A) is capable of connecting to the internet, either directly or indirectly through a network, to communicate information at the direction of an individual; and

Attachment #6

(B) has computer processing capabilities for collecting, sending, receiving, or analyzing data.

(10) COVERED DATA.—

(A) IN GENERAL.—The term "covered data" means information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual.

(B) LINKED OR REASONABLY LINKABLE.—For purposes of subparagraph (A), information held by a covered entity is linked or reasonably linkable to an individual or a device if, as a practical matter, it can be used on its own or in combination with other information held by, or readily accessible to, the covered entity to identify such individual or such device.

(C) EXCLUSIONS.—Such term does not include—

(i) aggregated data;

(ii) de-identified data;

(iii) employee data; or

(iv) publicly available information.

(D) AGGREGATED DATA.—For purposes of subparagraph (C), the term "aggregated data" means information that relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual.

(E) DE-IDENTIFIED DATA.—For purposes of subparagraph (C), the term "de-identified data" means information held by a covered entity that—

(i) does not identify, and is not linked or reasonably linkable to, an individual or device;

(ii) does not contain any persistent identifier or other information that could readily be used to reidentify the individual to whom, or the device to which, the identifier or information pertains;

(iii) is subject to a public commitment by the covered entity—

(I) to refrain from attempting to use such information to identify any individual or device; and

(II) to adopt technical and organizational measures to ensure that such information is not linked to any individual or device; and

(iv) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement that—

(I) the recipient of the information shall not use the information to identify any individual or device; and

(II) all onward disclosures of the information shall be subject to the requirement described in subclause (I).

(F) EMPLOYEE DATA.—For purposes of subparagraph (C), the term ‘‘employee data’’ means—

(i) information relating to an individual collected by a covered entity in the course of the individual acting as a job applicant to, or employee (regardless of whether such employee is paid or unpaid, or employed on a temporary basis), owner, director, officer, staff member, trainee, vendor, visitor, volunteer, intern, or contractor of, the entity, provided that such information is collected, processed, or transferred by the covered entity solely for purposes related to the individual's status as a current or former job applicant to, or an employee, owner, director, officer, staff member, trainee, vendor, visitor, volunteer, intern, or contractor of, that covered entity;

(ii) business contact information of an individual, including the individual's name, position or title, business telephone number, business address, business email address, qualifications, and other similar information, that is provided to a covered entity by an individual who is acting in a professional capacity, provided that such information is collected, processed, or transferred solely for purposes related to such individual's professional activities;

(iii) emergency contact information collected by a covered entity that relates to an individual who is acting in a role described in clause (i) with respect to the covered entity, provided that such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the individual; or

(iv) information relating to an individual (or a relative or beneficiary of such individual) that is necessary for the covered entity to collect, process, or transfer for the purpose of administering benefits to which such individual (or relative or beneficiary of such individual) is entitled on the basis of the individual acting in a role described in clause (i) with respect to the entity, provided that such information is collected, processed, or transferred solely for the purpose of administering such benefits.

(G) PUBLICLY AVAILABLE INFORMATION.—

(i) IN GENERAL.—For the purposes of subparagraph (C), the term "publicly available information" means any information that a covered entity has a reasonable basis to believe—

(I) has been lawfully made available to the general public from Federal, State, or local government records;

Attachment #6

(II) is widely available to the general public, including information from—

(aa) a telephone book or online directory;

(bb) television, internet, or radio content or programming; or

(cc) the news media or a website that is lawfully available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website); or

(III) is a disclosure to the general public that is required to be made by Federal, State, or local law.

(ii) EXCLUSIONS.—Such term does not include an obscene visual depiction (as defined for purposes of section 1460 of title 18, United States Code).

(11) COVERED ENTITY.—The term ''covered entity'' means any person that—

Attachment #6

(A) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or is—

(i) a common carrier described in section 5(a)(2) of such Act (15 U.S.C. 45(a)(2)); or

(ii) an organization not organized to carry on business for their own profit or that of their members;

(B) collects, processes, or transfers covered data; and

(C) determines the purposes and means of such collection, processing, or transfer.

(12) COVERED INTERNET PLATFORM.—

(A) IN GENERAL.—The term "covered internet platform" means any public-facing website, internet application, or mobile application, including a social network site, video sharing service, search engine, or content aggregation service.

(B) EXCLUSIONS.—Such term shall not include a platform that—

(i) is wholly owned, controlled, and operated by a person that—

(I) for the most recent 6-month period, did not employ more than 500 employees;

(II) for the most recent 3-year period, averaged less than $50,000,000 in annual gross receipts; and

(III) collects or processes on an annual basis the personal data of less than 1,000,000 individuals; or

(ii) is operated for the sole purpose of conducting research that is not made for profit either directly or indirectly.

(13) DATA BROKER.—

(A) IN GENERAL.—The term "data broker" means a covered entity whose principal source of revenue is derived from processing or transferring the covered data of individuals with whom the entity does not have a direct relationship on behalf of third parties for such third parties' use.

(B) EXCLUSION.—Such term does not include a service provider.

(14) DELETE.—The term "delete" means to remove or destroy information such that it is not

maintained in human or machine readable form and cannot be retrieved or utilized in such form in the normal course of business.

(15) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning set forth in section 105 of title 5, United States Code.

(16) INDEPENDENT REVIEW BOARD.—The term ''independent review board'' means a board, committee, or other group formally designated by a large online operator to review, to approve the initiation of, and to conduct periodic review of, any research by, or at the direction or discretion of a large online operator, involving human subjects.

(17) INDIVIDUAL.—The term ''individual'' means a natural person residing in the United States.

(18) INFERRED DATA.—The term ''inferred data'' means information that is created by a covered entity through the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(19) INFORMED CONSENT.—For purposes of section 206, the term ''informed consent''—

(A) means a process by which a research subject is provided adequate information prior to being included in any experiment or study to allow for an informed decision about voluntary participation in a behavioral or psychological research experiment or study, while ensuring the understanding of the potential participant of the furnished information and any associated benefits, risks, or consequences of participation prior to obtaining the voluntary agreement to participate by the participant; and

(B) does not include—

(i) the consent of an individual under the age of 13; or

(ii) the consent to a provision contained in a general contract or service agreement.

(20) INPUT-TRANSPARENT ALGORITHM.—

(A) IN GENERAL.—For purposes of section 205, the term "input-transparent algorithm" means an algorithmic ranking system that does not use the user-specific data of a user to determine the order or manner that information is furnished to such user on a covered internet platform, unless the user-specific data is expressly provided to the platform by the user for such purpose.

Attachment #6

(B) INCLUSION OF AGE-APPROPRIATE CONTENT FILTERS.—Such term shall include an algorithmic ranking system that uses user-specific data to determine whether a user is old enough to access age-restricted content on a covered internet platform, provided that the system otherwise meets the requirements of subparagraph (A).

(C) DATA PROVIDED FOR EXPRESS PURPOSE OF INTERACTION WITH PLATFORM.—For purposes of subparagraph (A), user-specific data that is provided by a user for the express purpose of determining the order or manner that information is furnished to a user on a covered internet platform—

(i) shall include user-supplied search terms, filters, speech patterns (if provided for the purpose of enabling the platform to accept spoken input or selecting the language in which the user interacts with the platform), saved preferences, and the user's current geographical location;

(ii) shall include data supplied to the platform by the user that expresses the user's desire that information be furnished to them, such as the social media profiles the user follows, the video channels the user subscribes to, or other sources of content on the platform the user follows;

(iii) shall not include the history of the user's connected device, including the user's history of web searches and browsing, geographical locations, physical activity, device interaction, and financial transactions; and

(iv) shall not include inferences about the user or the user's connected device, without regard to whether such inferences are based on data described in clause (i).

(21) LARGE DATA HOLDER.—The term ''large data holder'' means a covered entity that in the most recent calendar year—

(A) processed or transferred the covered data of more than 8,000,000 individuals; or

(B) processed or transferred the sensitive covered data of more than 300,000 individuals or devices that are linked or reasonably linkable to an individual (excluding any instance where the covered entity processes the log-in information of an individual or device to allow the indi-

Attachment #6

vidual or device to log in to an account administered by the covered entity).

(22) LARGE ONLINE OPERATOR.—For purposes of section 206, the term "large online operator" means any person that—

(A) provides an online service;

(B) has more than 100,000,000 authenticated users of an online service in any 30-day period; and

(C) is subject to the jurisdiction of the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(23) MATERIAL.—The term "material" means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals), that such act, practice, or representation is likely to affect an individual's decision or conduct regarding a product or service.

(24) ONLINE SERVICE.—For purposes of section 206, the term "online service" means a website or a service, other than an internet access service, that is made available to the public over the internet, including a social network, a search engine, or email service.

(25) OPAQUE ALGORITHM.—

(A) IN GENERAL.—The term "opaque algorithm" means an algorithmic ranking system that determines the order or manner that information is furnished to a user on a covered internet platform based, in whole or part, on user-specific data that was not expressly provided by the user to the platform for such purpose.

(B) EXCEPTION FOR AGE-APPROPRIATE CONTENT FILTERS.—Such term shall not include an algorithmic ranking system used by a covered internet platform if—

(i) the only user-specific data (including inferences about the user) that the system uses is information relating to the age of the user; and

(ii) such information is only used to restrict a user's access to content on the basis that the individual is not old enough to access such content.

(26) PROCESS.—The term "process" means any operation or set of operations performed on covered data including analysis, organization, struc-

turing, retaining, using, or otherwise handling covered data.

(27) PROCESSING PURPOSE.—The term "processing purpose" means a reason for which a covered entity processes covered data.

(28) RESEARCH.—The term "research" means the scientific analysis of information, including covered data, by a covered entity or those with whom the covered entity is cooperating or others acting at the direction or on behalf of the covered entity, that is conducted for the primary purpose of advancing scientific knowledge and may be for the commercial benefit of the covered entity.

(29) SEARCH SYNDICATION CONTRACT; UPSTREAM PROVIDER; DOWNSTREAM PROVIDER.—

(A) SEARCH SYNDICATION CONTRACT.—The term "search syndication contract" means a contract or subcontract for the sale, license, or other right to access an index of web pages on the internet for the purpose of operating an internet search engine.

(B) UPSTREAM PROVIDER.—The term "upstream provider" means, with respect to a search syndication contract, the person that grants access to an index of web pages on the internet to a downstream provider under the contract.

(C) DOWNSTREAM PROVIDER.—The term ''downstream provider'' means, with respect to a search syndication contract, the person that receives access to an index of web pages on the internet from an upstream provider under such contract.

(30) SENSITIVE COVERED DATA.—

(A) IN GENERAL.—The term ''sensitive covered data'' means any of the following forms of covered data of an individual:

(i) A unique, government-issued identifier, such as a Social Security number, passport number, or driver's license number, that is not required to be displayed to the public.

(ii) Any covered data that describes or reveals the diagnosis or treatment of the past, present, or future physical health, mental health, or disability of an individual.

(iii) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.

(iv) Covered data that is biometric information.

(v) A persistent identifier.

(vi) Precise geolocation information.

(vii) The contents of an individual's private communications, such as emails, texts, direct messages, or mail, or the identity of the parties subject to such communications, unless the covered entity is the intended recipient of the communication.

(viii) Account log-in credentials such as a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(ix) Covered data revealing an individual's racial or ethnic origin, or religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information.

(x) Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information.

(xi) Covered data about the online activities of an individual that addresses or reveals a category of covered data described in another subparagraph of this paragraph.

(xii) Covered data that is calendar information, address book information, phone or text logs, photos, or videos maintained for private use on an individual's device.

(xiii) Any covered data collected or processed by a covered entity for the purpose of identifying covered data described in another paragraph of this paragraph.

(xiv) Any other category of covered data designated by the Commission pursuant to a rulemaking under section 553 of title 5, United States Code.

(B) BIOMETRIC INFORMATION.—For purposes of subparagraph (A), the term ''biometric information''—

(i) means the physiological or biological characteristics of an individual, including deoxyribonucleic acid, that are used, singly or in combination with each other or with other identifying data, to establish the identity of an individual; and

(ii) includes—

(I) imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; and

(II) keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(C) PERSISTENT IDENTIFIER.—For purposes of subparagraph (A), the term ''persistent identifier'' means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol address, a processor or device serial number, or another unique device identifier.

(D) PRECISE GEOLOCATION INFORMATION.—For purposes of subparagraph (A), the term ''precise geolocation information'' means technologically derived information capable of determining the past or present actual physical location of an individual or an individual's device at a specific point in time to within 1,750 feet.

(31) SERVICE PROVIDER.—The term ''service provider'' means, with respect to a set of covered data, a covered entity that processes or transfers such covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of, another covered entity that—

(A) is not related to the covered entity providing the service or function by common ownership or corporate control; and

(B) does not share common branding with the covered entity providing the service or function.

(32) SERVICE PROVIDER DATA.—The term ''service provider data'' means, with respect to a set of covered data and a service provider, covered data

that is collected by the service provider on behalf of a covered entity or transferred to the service provider by a covered entity for the purpose of allowing the service provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(33) THIRD PARTY.—The term "third party" means, with respect to a set of covered data, a covered entity—

(A) that is not a service provider with respect to such covered data; and

(B) that received such covered data from another covered entity—

(i) that is not related to the covered entity by common ownership or corporate control; and

(ii) that does not share common branding with the covered entity.

(34) THIRD PARTY DATA.—The term "third party data" means, with respect to a third party, covered data that has been transferred to the third party by a covered entity.

(35) TRANSFER.—The term "transfer" means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any

other means for consideration of any kind or for a commercial purpose.

(36) USER DATA.—For purposes of section 206, the term ''user data'' means any information relating to an identified or identifiable individual user, whether directly submitted to the large online operator by the user, or derived from the observed activity of the user by the large online operator.

(37) USER-SPECIFIC DATA.—For purposes of section 205, the term ''user-specific data'' means information relating to an individual or a specific connected device that would not necessarily be true of every individual or device.

SEC. 3. EFFECTIVE DATE.

Except as otherwise provided in this Act, this Act shall take effect 18 months after the date of enactment of this Act.

TITLE I—INDIVIDUAL CONSUMER DATA RIGHTS

SEC. 101. CONSUMER LOYALTY.

(a) PROHIBITION ON THE DENIAL OF PRODUCTS OR SERVICES.—

(1) IN GENERAL.—Subject to paragraph (2), a covered entity shall not deny products or services to an individual because the individual exercises a right

established under subparagraph (A), (B), or (D) of section 103(a)(1).

(2) RULES OF APPLICATION.—A covered entity—

(A) shall not be in violation of paragraph (1) with respect to a product or service and an individual if the exercise of a right described in such paragraph by the individual precludes the covered entity from providing such product or service to such individual; and

(B) may offer different types of pricing and functionalities with respect to a product or service based on an individual's exercise of a right described in such paragraph.

(b) NO WAIVER OF INDIVIDUAL CONTROLS.—The rights and obligations created under section 103 may not be waived in an agreement between a covered entity and an individual.

SEC. 102. TRANSPARENCY.

(a) IN GENERAL.—A covered entity that processes covered data shall, with respect to such data, publish a privacy policy that is—

(1) disclosed, in a clear and conspicuous manner, to an individual prior to or at the point of the collection of covered data from the individual; and

(2) made available, in a clear and conspicuous manner, to the public.

(b) CONTENT OF PRIVACY POLICY.—The privacy policy required under subsection (a) shall include the following:

(1) The identity and the contact information of the covered entity (including the covered entity's points of contact for privacy and data security inquiries) and the identity of any affiliate to which covered data may be transferred by the covered entity.

(2) The categories of covered data the covered entity collects.

(3) The processing purposes for each category of covered data the covered entity collects.

(4) Whether the covered entity transfers covered data, the categories of recipients to whom the covered entity transfers covered data, and the purposes of the transfers.

(5) A general description of the covered entity's data retention practices for covered data and the purposes for such retention.

(6) How individuals can exercise their rights under section 103.

(7) A general description of the covered entity's data security practices.

(8) The effective date of the privacy policy.

(c) LANGUAGES.—A privacy policy required under subsection (a) shall be made available in all of the languages in which the covered entity provides a product or service that is subject to the policy, or carries out activities related to such product or service.

(d) MATERIAL CHANGES.—If a covered entity makes a material change to its privacy policy, it shall notify the individuals affected before further processing or transferring of previously collected covered data and provide an opportunity to withdraw consent to further processing or transferring of the covered data under the changed policy. The covered entity shall provide direct notification, where possible, regarding a material change to the privacy policy to affected individuals, taking into account available technology and the nature of the relationship.

(e) APPLICATION TO INDIRECT TRANSFERS.—Where the ownership of an individual's device is transferred directly from one individual to another individual, a covered entity may satisfy its obligation to disclose a privacy policy prior to or at the point of collection of covered data by making the privacy policy available under (a)(2).

SEC. 103. INDIVIDUAL CONTROL.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3), a covered entity shall provide an individual, immediately or as quickly as possible and in no case later than 90 days after receiving a verified request from the individual, with the right to reasonably—

(A) access—

(i) the covered data of the individual, or an accurate representation of the covered data of the individual, that is or has been processed by the covered entity or any service provider of the covered entity;

(ii) if applicable, a list of categories of third parties and service providers to whom the covered entity has transferred the covered data of the individual; and

(iii) if a covered entity transfers covered data, a description of the purpose for which the covered entity transferred the covered data of the individual to a service provider or third party;

(B) request that the covered entity—

(i) correct material inaccuracies or materially incomplete information with re-

Attachment #6

spect to the covered data of the individual that is maintained by the covered entity; and

(ii) notify any service provider or third party to which the covered entity transferred such covered data of the corrected information;

(C) request that the covered entity—

(i) either delete or deidentify covered data of the individual that is or has been maintained by the covered entity; and

(ii) notify any service provider or third party to which the covered entity transferred such covered data of the individual's request, unless the transfer of such data to the third party was made at the direction of the individual; and

(D) to the extent that is technically feasible, provide covered data of the individual that is or has been generated and submitted to the covered entity by the individual and maintained by the covered entity in a portable, structured, and machine-readable format that is not subject to licensing restrictions.

Attachment #6

(2) FREQUENCY AND COST OF ACCESS.—A covered entity shall—

(A) provide an individual with the opportunity to exercise the rights described in paragraph (1) not less than twice in any 12-month period; and

(B) with respect to the first 2 times that an individual exercises the rights described in paragraph (1) in any 12-month period, allow the individual to exercise such rights free of charge.

(3) EXCEPTIONS.—A covered entity—

(A) shall not comply with a request to exercise the rights described in paragraph (1) if the covered entity cannot verify that the individual making the request is the individual to whom the covered data that is the subject of the request relates;

(B) may decline to comply with a request that would—

(i) require the covered entity to retain any covered data for the sole purpose of fulfilling the request;

(ii) be impossible or demonstrably impracticable to comply with; or

(iii) require the covered entity to combine, relink, or otherwise reidentify covered data that has been deidentified;

(iv) result in the release of trade secrets, or other proprietary or confidential data or business practices;

(v) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, or investigate malicious or unlawful activity, or enforce contracts;

(vi) require disproportionate effort, taking into consideration available technology, or would not be reasonably feasible on technical grounds;

(vii) compromise the privacy, security, or other rights of the covered data of another individual;

(viii) be excessive or abusive to another individual; or

(ix) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States; and

(C) may delete covered data instead of providing access and correction rights under subparagraphs (A) and (B) of paragraph (1) if such covered data—

(i) is not sensitive covered data; and

(ii) is used only for the purposes of contacting individuals with respect to marketing communications.

(b) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing requirements for covered entities with respect to the verification of requests to exercise rights described in subsection (a)(1).

SEC. 104. RIGHTS TO CONSENT.

(a) CONSENT.—Except as provided in section 108, a covered entity shall not, without the prior, affirmative express consent of an individual—

(1) transfer sensitive covered data of the individual to a third party; or

(2) process sensitive covered data of the individual.

(b) REQUIREMENTS FOR AFFIRMATIVE EXPRESS CONSENT.—In obtaining the affirmative express consent of an individual to process the sensitive covered data of

Attachment #6

the individual as required under subsection (a)(2), a covered entity shall provide the individual with notice that shall—

(1) include a clear description of the processing purpose for which the sensitive covered data will be processed;

(2) clearly identify any processing purpose that is necessary to fulfill a request made by the individual;

(3) include a prominent heading that would enable a reasonable individual to easily identify the processing purpose for which consent is sought; and

(4) clearly explain the individual's right to provide or withhold consent.

(c) REQUIREMENTS RELATED TO MINORS.—A covered entity shall not transfer the covered data of an individual to a third-party without affirmative express consent from the individual or the individual's parent or guardian if the covered entity has actual knowledge that the individual is between 13 and 16 years of age.

(d) RIGHT TO OPT OUT.—Except as provided in section 108, a covered entity shall provide an individual with the ability to opt out of the collection, processing, or transfer of such individual's covered data before such collection, processing, or transfer occurs.

Attachment #6

(e) PROHIBITION ON INFERRED CONSENT.—A covered entity shall not infer that an individual has provided affirmative express consent to a processing purpose from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(f) WITHDRAWAL OF CONSENT.—A covered entity shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent.

(g) RULEMAKING.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to establish requirements for covered entities regarding clear and conspicuous procedures for allowing individuals to provide or withdraw affirmative express consent for the collection of sensitive covered data.

SEC. 105. MINIMIZING DATA COLLECTION, PROCESSING, AND RETENTION.

(a) IN GENERAL.—A covered entity shall not collect, process, or transfer covered data beyond—

(1) what is reasonably necessary, proportionate, and limited to provide or improve a product, service, or a communication about a product or service, including what is reasonably necessary, proportionate, and limited to provide a product or service specifically requested by an individual or reasonably antici-

pated within the context of the covered entity's ongoing relationship with an individual;

(2) what is reasonably necessary, proportionate, or limited to otherwise process or transfer covered data in a manner that is described in the privacy policy that the covered entity is required to publish under section 102(a); or

(3) what is expressly permitted by this Act or any other applicable Federal law.

(b) BEST PRACTICES.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of covered data in accordance with this section.

(c) RULE OF CONSTRUCTION.—Notwithstanding section 405 of this Act, nothing in this section supersedes any other provision of this Act or other applicable Federal law.

SEC. 106. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall not process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider;

Attachment #6

(2) shall not transfer service provider data to a third party for any purpose other than a purpose performed on behalf of, or at the direction of, the covered entity that transferred the data to the service provider without the affirmative express consent of the individual to whom the service provider data relates;

(3) at the direction of the covered entity that transferred service provider data to the service provider, shall delete or deidentify such data—

(A) as soon as practicable after the service provider has completed providing the service or function for which the data was transferred to the service provider; or

(B) as soon as practicable after the end of the period during which the service provider is to provide services with respect to such data, as agreed to by the service provider and the covered entity that transferred the data;

(4) is exempt from the requirements of section 103 with respect to service provider data, but shall, to the extent practicable—

(A) assist the covered entity from which it received the service provider data in fulfilling

Attachment #6

requests to exercise rights under section 103(a); and

(B) upon receiving notice from a covered entity of a verified request made under section 103(a)(1) to delete, deidentify, or correct service provider data held by the service provider, delete, deidentify, or correct such data; and

(5) is exempt from the requirements of sections 104 and 105.

(b) THIRD PARTIES.—A third party—

(1) shall not process third party data for a processing purpose inconsistent with the reasonable expectation of the individual to whom such data relates;

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred third party data regarding the reasonable expectations of individuals to whom such data relates, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) is exempt from the requirements of sections 104 and 105.

Attachment #6

(c) BANKRUPTCY.—In the event that a covered entity enters into a bankruptcy proceeding which would lead to the disclosure of covered data to a third party, the covered entity shall in a reasonable time prior to the disclosure—

(1) provide notice of the proposed disclosure of covered data, including the name of the third party and their policies and practices with respect to the covered data, to all affected individuals; and

(2) provide each affected individual with the opportunity to withdraw any previous affirmative express consent related to the covered data of the individual or request the deletion or deidentification of the covered data of the individual.

(d) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity shall exercise reasonable due diligence to ensure compliance with this section before—

(A) selecting a service provider; or

(B) deciding to transfer covered data to a third party.

(2) GUIDANCE.—Not later than 2 years after the effective date of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent prac-

ticable, minimize unreasonable burdens on small- and medium-sized covered entities.

SEC. 107. PRIVACY IMPACT ASSESSMENTS.

(a) PRIVACY IMPACT ASSESSMENTS OF NEW OR MATERIAL CHANGES TO PROCESSING OF COVERED DATA.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act (or, if later, not later than 1 year after a covered entity first meets the definition of a large data holder (as defined in section 2)), each covered entity that is a large data holder shall conduct a privacy impact assessment of each of their processing activities involving covered data that present a heightened risk of harm to individuals, and each such assessment shall weigh the benefits of the covered entity's covered data collection, processing, and transfer practices against the potential adverse consequences to individual privacy of such practices.

(2) ASSESSMENT REQUIREMENTS.—A privacy impact assessment required under paragraph (1)—

(A) shall be reasonable and appropriate in scope given—

(i) the nature of the covered data collected, processed, or transferred by the covered entity;

Attachment #6

(ii) the volume of the covered data collected, processed, or transferred by the covered entity;

(iii) the size of the covered entity; and

(iv) the potential risks posed to the privacy of individuals by the collection, processing, or transfer of covered data by the covered entity;

(B) shall be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under subsection (b); and

(C) shall be approved by the data privacy officer of the covered entity.

(b) ONGOING PRIVACY IMPACT ASSESSMENTS.—

(1) IN GENERAL.—A covered entity that is a large data holder shall, not less frequently than once every 2 years after the covered entity conducted the privacy impact assessment required under subsection (a), conduct a privacy impact assessment of the collection, processing, and transfer of covered data by the covered entity to assess the extent to which—

(A) the ongoing practices of the covered entity are consistent with the covered entity's published privacy policies and other representa-

Attachment #6

tions that the covered entity makes to individuals;

(B) any customizable privacy settings included in a service or product offered by the covered entity are adequately accessible to individuals who use the service or product and are effective in meeting the privacy preferences of such individuals;

(C) the practices and privacy settings described in subparagraphs (A) and (B), respectively—

(i) meet the expectations of a reasonable individual; and

(ii) provide an individual with adequate control over the individual's covered data;

(D) the covered entity could enhance the privacy and security of covered data through technical or operational safeguards such as encryption, deidentification, and other privacy-enhancing technologies; and

(E) the processing of covered data is compatible with the stated purposes for which it was collected.

(2) Approval by data privacy officer.—The data privacy officer of a covered entity shall approve the findings of an assessment conducted by the covered entity under this subsection.

SEC. 108. SCOPE OF COVERAGE.

(a) General Exceptions.—Notwithstanding any provision of this title other than subsections (a) through (c) of section 102, a covered entity may collect, process or transfer covered data for any of the following purposes, provided that the collection, processing, or transfer is reasonably necessary, proportionate, and limited to such purpose:

(1) To initiate or complete a transaction or to fulfill an order or provide a service specifically requested by an individual, including associated routine administrative activities such as billing, shipping, financial reporting, and accounting.

(2) To perform internal system maintenance, diagnostics, product or service management, inventory management, and network management.

(3) To prevent, detect, or respond to a security incident or trespassing, provide a secure environment, or maintain the safety and security of a product, service, or individual.

(4) To protect against malicious, deceptive, fraudulent, or illegal activity.

(5) To comply with a legal obligation or the establishment, exercise, analysis, or defense of legal claims or rights, or as required or specifically authorized by law.

(6) To comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by an Executive agency.

(7) To cooperate with an Executive agency or a law enforcement official acting under the authority of an Executive or State agency concerning conduct or activity that the Executive agency or law enforcement official reasonably and in good faith believes may violate Federal, State, or local law, or pose a threat to public safety or national security.

(8) To address risks to the safety of an individual or group of individuals, or to ensure customer safety, including by authenticating individuals in order to provide access to large venues open to the public.

(9) To effectuate a product recall pursuant to Federal or State law.

(10) To conduct public or peer-reviewed scientific, historical, or statistical research that—

Attachment #6

(A) is in the public interest;

(B) adheres to all applicable ethics and privacy laws; and

(C) is approved, monitored, and governed by an institutional review board or other oversight entity that meets standards promulgated by the Commission pursuant to section 553 of title 5, United States Code.

(11) To transfer covered data to a service provider.

(12) For a purpose identified by the Commission pursuant to a regulation promulgated under subsection (b).

(b) ADDITIONAL PURPOSES.—The Commission may promulgate regulations under section 553 of title 5, United States Code, identifying additional purposes for which a covered entity may collect, process or transfer covered data.

(c) SMALL BUSINESS EXCEPTION.—Sections 103, 105, and 301 shall not apply in the case of a covered entity that can establish that, for the 3 preceding calendar years (or for the period during which the covered entity has been in existence if such period is less than 3 years)—

(1) the covered entity's average annual gross revenues did not exceed $50,000,000;

Attachment #6

(2) on average, the covered entity annually processed the covered data of less than 1,000,000 individuals;

(3) the covered entity never employed more than 500 individuals at any one time; and

(4) the covered entity derived less than 50 percent of its revenues from transferring covered data.

TITLE II—DATA TRANSPARENCY, INTEGRITY, AND SECURITY

SEC. 201. ALGORITHM BIAS, DETECTION, AND MITIGATION.

(a) FTC ENFORCEMENT ASSISTANCE.—

(1) IN GENERAL.—Whenever the Commission obtains information that a covered entity may have processed or transferred covered data in violation of Federal anti-discrimination laws, the Commission shall transmit such information (excluding any such information that is a trade secret as defined by section 1839 of title 18, United States Code) to the appropriate Executive agency or State agency with authority to initiate proceedings relating to such violation.

(2) ANNUAL REPORT.—Beginning in 2021, the Commission shall submit an annual report to Congress that includes—

(A) a summary of the types of information the Commission transmitted to Executive agencies or State agencies during the preceding year pursuant to this subsection; and

(B) a summary of how such information relates to Federal anti-discrimination laws.

(3) COOPERATION WITH OTHER AGENCIES.—The Commission may implement this subsection by executing agreements or memoranda of understanding with the appropriate Executive agencies.

(4) RELATIONSHIP TO OTHER LAWS.—Notwithstanding section 405, nothing in this subsection shall supersede any other provision of law.

(b) ALGORITHM TRANSPARENCY REPORTS.—

(1) STUDY AND REPORT.—

(A) STUDY.—The Commission shall conduct a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), examining the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws.

(B) REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission shall publish a report containing the re-

Attachment #6

sults of the study required under subparagraph (A).

(C) GUIDANCE.—The Commission shall use the results of the study described in paragraph (A) to develop guidance to assist covered entities in avoiding the discriminatory use of algorithms.

(2) UPDATED REPORT.—Not later than 5 years after the publication of the report required under paragraph (1), the Commission shall publish an updated report.

SEC. 202. DIGITAL CONTENT FORGERIES.

(a) DEFINITION.—Not later than 6 months after the date of enactment of this Act, the National Institute of Standards and Technology shall develop and publish a definition of ''digital content forgery'' and accompanying explanatory materials.

(b) ELEMENTS OF DEFINITION.—In developing a definition of ''digital content forgery'' under subsection (a), the National Institute of Standards and Technology shall consider the following factors:

(1) Whether the content is created with the intent to deceive an individual into believing the content was genuine.

(2) Whether the content is genuine or manipulated.

(3) The impression the content makes on a reasonable individual that observes the content.

(4) Whether the production of the content was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.

(5) The scope of technologies that may be utilized during the creation or publication of digital content forgeries, including—

(A) video recording or film;

(B) sound recording;

(C) electronic image or photograph; or

(D) any digital representation of speech or conduct.

(c) SCOPE OF DEFINITION.—The definition published by the National Institute of Standards and Technology under subsection (a) shall not supersede any other provision of law or be construed to limit the authority of any Executive agency related to digital content forgeries.

(d) COMMISSION REPORTS.—

(1) INITIAL REPORT.—Not later than 1 year after the National Institute of Standards and Technology publishes the definition and materials re-

quired under subsection (a), the Commission shall publish a report regarding the impact of digital content forgeries on individuals and competition.

(2) SUBSEQUENT REPORTS.—Not later than 2 years after the publication of the report required under paragraph (1), and as often as the Commission shall deem necessary thereafter, the Commission shall publish an updated version of such report.

(3) CONTENT OF REPORTS.—Each report required under this subsection shall include—

(A) a description of the types of digital content forgeries, including those used to commit fraud, cause adverse consequences, violate any provision of law enforced by the Commission, or violate civil rights recognized under Federal law;

(B) a description of the common sources in the United States of digital content forgeries and commercial sources of digital content forgery technologies;

(C) an assessment of the uses, applications, and adverse consequences of digital content forgeries, including the impact of digital content forgeries on individuals, digital identity, and competition;

(D) an analysis of the methods available to individuals to identify digital content forgeries as well as a description of commercial technological counter-measures that are, or could be, used to address concerns with digital content forgeries, which may include counter-measures that warn individuals of suspect content;

(E) a description of any remedies available to protect an individual's identity and reputation from adverse consequences caused by digital content forgeries, such as protections or remedies available under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or any other law; and

(F) any additional information the Commission determines appropriate.

(e) ESTABLISHMENT OF DIGITAL CONTENT FORGERY PRIZE COMPETITION.—Not later than 1 year after the date of enactment of this Act, the Director of the National Institute of Standards and Technology, in coordination with the Commission, shall establish under section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) a prize competition to spur the development of technical solutions to assist individuals and

Attachment #6

the public in identifying digital content forgeries and related technologies.

SEC. 203. DATA BROKERS.

(a) In General.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker, such covered entity shall register with the Commission pursuant to the requirements of this section.

(b) Registration Requirements.—In registering with the Commission as required under subsection (a), a data broker shall do the following:

(1) Pay to the Commission a registration fee of $100.

(2) Provide the Commission with the following information:

(A) The name and primary physical, email, and internet addresses of the data broker.

(B) Any additional information or explanation the data broker chooses to provide concerning its data collection and processing practices.

(c) Penalties.—A data broker that fails to register as required under subsection (a) shall be liable for—

(1) a civil penalty of $50 for each day it fails to register, not to exceed a total of $10,000 for each year; and

(2) an amount equal to the fees due under this section for each year that it failed to register as required under subsection (a).

(d) PUBLICATION OF REGISTRATION INFORMATION.—The Commission shall publish on the internet website of the Commission the registration information provided by data brokers under this section.

SEC. 204. PROTECTION OF COVERED DATA.

(a) IN GENERAL.—A covered entity shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of covered data.

(b) DATA SECURITY REQUIREMENTS.—The data security policies and practices required under subsection (a) shall be—

(1) appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's collection or processing of covered data, the volume and nature of the covered data at issue, and the cost of available tools to improve security and reduce vulnerabilities; and

(2) designed to—

(A) identify and assess vulnerabilities to covered data;

(B) take reasonable preventative and corrective action to address known vulnerabilities to covered data; and

(C) detect, respond to, and recover from cybersecurity incidents related to covered data.

(c) RULEMAKING AND GUIDANCE.—

(1) RULEMAKING AUTHORITY AND SCOPE.—

(A) IN GENERAL.—The Commission may, pursuant to a proceeding in accordance with section 553 of title 5, United States Code, issue regulations to identify processes for receiving and assessing information regarding vulnerabilities to covered data that are reported to the covered entity.

(B) CONSULTATION WITH NIST.—In promulgating regulations under this paragraph, the Commission shall consult with, and take into consideration guidance from, the National Institute for Standards and Technology

(2) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance to covered entities on how to—

Attachment #6

(A) identify and assess vulnerabilities to covered data, including—

(i) the potential for unauthorized access to covered data;

(ii) vulnerabilities in the covered entity's collection or processing of covered data;

(iii) the management of access rights; and

(iv) the use of service providers to process covered data;

(B) take reasonable preventative and corrective action to address vulnerabilities to covered data; and

(C) detect, respond to, and recover from cybersecurity incidents and events.

(d) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), and is in compliance with the information security requirements of such Act, shall be deemed to be in compliance with the requirements of this section with respect to

Attachment #6

covered data that is subject to the requirements of such Act.

SEC. 205. FILTER BUBBLE TRANSPARENCY.

(a) IN GENERAL.—Beginning on the date that is 1 year after the date of enactment of this Act, it shall be unlawful—

(1) for any person to operate a covered internet platform that uses an opaque algorithm unless the person complies with the requirements of subsection (b); or

(2) for any upstream provider to grant access to an index of web pages on the internet under a search syndication contract that does not comply with the requirements of subsection (c).

(b) OPAQUE ALGORITHM REQUIREMENTS.—

(1) IN GENERAL.—The requirements of this subsection with respect to a person that operates a covered internet platform that uses an opaque algorithm are the following:

(A) The person provides notice to users of the platform that the platform uses an opaque algorithm that makes inferences based on user-specific data to select the content the user sees. Such notice shall be presented in a clear, conspicuous manner on the platform whenever the user interacts with an opaque algorithm for the first time, and may be a one-time notice that can be dismissed by the user.

(B) The person makes available a version of the platform that uses an input-transparent algorithm and enables users to easily switch between the version of the platform that uses an opaque algorithm and the version of the platform that uses the input-transparent algorithm by selecting a prominently placed icon, which shall be displayed wherever the user interacts with an opaque algorithm.

(2) NONAPPLICATION TO CERTAIN DOWNSTREAM PROVIDERS.—Paragraph (1) shall not apply with respect to an internet search engine if—

(A) the search engine is operated by a downstream provider with fewer than 1,000 employees; and

(B) the search engine uses an index of web pages on the internet to which such provider received access under a search syndication contract.

(c) SEARCH SYNDICATION CONTRACT REQUIREMENT.—The requirements of this subsection with respect to a search syndication contract are that—

Attachment #6

(1) as part of the contract, the upstream provider makes available to the downstream provider the same input-transparent algorithm used by the upstream provider for purposes of complying with subsection (b)(1)(B); and

(2) the upstream provider does not impose any additional costs, degraded quality, reduced speed, or other constraint on the functioning of such algorithm when used by the downstream provider to operate an internet search engine relative to the performance of such algorithm when used by the upstream provider to operate an internet search engine.

SEC. 206. UNFAIR AND DECEPTIVE ACTS AND PRACTICES RELATING TO THE MANIPULATION OF USER INTERFACES.

(a) CONDUCT PROHIBITED.—

(1) IN GENERAL.—It shall be unlawful for any large online operator—

(A) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data;

(B) to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved; or

(C) to design, modify, or manipulate a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of 13, with the purpose or substantial effect of cultivating compulsive usage, including video auto-play functions initiated without the consent of a user.

(b) DUTIES OF LARGE ONLINE OPERATORS.—Any large online operator that engages in any form of behavioral or psychological research based on the activity or data of its users shall—

(1) disclose to its users on a routine basis, but not less than once each 90 days, any experiments or studies that user was subjected to or enrolled in with the purpose of promoting engagement or product conversion;

(2) disclose to the public on a routine basis, but not less than once each 90 days, any experiments or studies with the purposes of promoting engagement

or product conversion being currently undertaken, or concluded since the prior disclosure;

(3) shall present the disclosures in paragraphs (1) and (2) in a manner that—

(A) is clear, conspicuous, context-appropriate, and easily accessible; and

(B) is not deceptively obscured;

(4) establish an Independent Review Board for any behavioral or psychological research, of any purpose, conducted on users or on the basis of user activity or data, which shall review and have authority to approve, require modification in, or disapprove all behavioral or psychological experiments or research; and

(5) ensure that any Independent Review Board established under paragraph (4) shall register with the Commission, including providing to the Commission—

(A) the names and resumes of every board member;

(B) the composition and reporting structure of the Board to the management of the operator;

(C) the process by which the Board is to be notified of proposed studies or modifications along with the processes by which the Board is capable of vetoing or amending such proposals;

(D) any compensation provided to board members; and

(E) any conflict of interest that might exist concerning a board member's participation in the Board.

(c) REGISTERED PROFESSIONAL STANDARDS BODY.—

(1) IN GENERAL.—An association of large online operators may register as a professional standards body by filing with the Commission an application for registration in such form as the Commission, by rule, may prescribe containing the rules of the association and such other information and documents as the Commission, by rule, may prescribe as necessary or appropriate in the public interest or for protecting the welfare of users of large online operators.

(2) PROFESSIONAL STANDARDS BODY.—An association of large online operators may not register as a professional standards body unless the Commission determines that—

(A) the association is so organized and has the capacity to enforce compliance by its members and persons associated with its members, with the provisions of this Act;

(B) the rules of the association provide that any large online operator may become a member of such association;

(C) the rules of the association assure a fair representation of its members in the selection of its directors and administration of its affairs and provide that one or more directors shall be representative of users and not be associated with, or receive any direct or indirect funding from, a member of the association or any large online operator;

(D) the rules of the association are designed to prevent exploitative and manipulative acts or practices, to promote transparent and fair principles of technology development and design, to promote research in keeping with best practices of study design and informed consent, and to continually evaluate industry practices and issue binding guidance consistent with the objectives of this Act;

(E) the rules of the association provide that its members and persons associated with its members shall be appropriately disciplined

Attachment #6

for violation of any provision of this Act, the rules or regulations thereunder, or the rules of the association, by expulsion, suspension, limitation of activities, functions, fine, censure, being suspended or barred from being associated with a member, or any other appropriate sanction; and

(F) the rules of the association are in accordance with the provisions of this Act, and, in general, provide a fair procedure for the disciplining of members and persons associated with members, the denial of membership to any person seeking membership therein, the barring of any person from becoming associated with a member thereof, and the prohibition or limitation by the association of any person with respect to access to services offered by the association or a member thereof.

(3) RESPONSIBILITIES AND ACTIVITIES.—

(A) BRIGHT-LINE RULES.—An association shall develop, on a continuing basis, guidance and bright-line rules for the development and design of technology products of large online operators consistent with subparagraph (B).

Attachment #6

(B) Safe harbors.—In formulating guidance under subparagraph (A), the association shall define conduct that does not have the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice, or of cultivating compulsive usage for children such as—

(i) de minimis user interface changes derived from testing consumer preferences, including different styles, layouts, or text, where such changes are not done with the purpose of obtaining user consent or user data;

(ii) algorithms or data outputs outside the control of a large online operator or its affiliates; and

(iii) establishing default settings that provide enhanced privacy protection to users or otherwise enhance their autonomy and decision-making ability.

(d) Enforcement by the Commission.—

(1) Unfair or deceptive acts or practice.—A violation of subsection (a) or (b) shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B)

Attachment #6

of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) DETERMINATION.—For purposes of enforcement of this Act, the Commission shall determine an act or practice is unfair or deceptive if the act or practice—

(A) has the purpose, or substantial effect, of subverting or impairing user autonomy, decision-making, or choice to obtain consent or user data; or

(B) has the purpose, or substantial effect, of cultivating compulsive usage by a child under 13.

(3) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that—

(A) establish rules and procedures for obtaining the informed consent of users;

(B) establish rules for the registration, formation, oversight, and management of the independent review boards, including standards that ensure effective independence of such entities from improper or undue influence by a large online operator;

Attachment #6

(C) establish rules for the registration, formation, oversight, and management of professional standards bodies, including procedures for the regular oversight of such bodies and revocation of their designation; and

(D) in consultation with a professional standards body established under subsection (c), define conduct that does not have the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice, or of cultivating compulsive usage for children such as—

(i) de minimis user interface changes derived from testing consumer preferences, including different styles, layouts, or text, where such changes are not done with the purpose of obtaining user consent or user data;

(ii) algorithms or data outputs outside the control of a large online operator or its affiliates; and

(iii) establishing default settings that provide enhanced privacy protection to users or otherwise enhance their autonomy and decision-making ability.

(4) SAFE HARBOR.—The Commission may not bring an enforcement action under this section against any large online operator that relied in good faith on the guidance of a professional standards body.

TITLE III—CORPORATE ACCOUNTABILITY

SEC. 301. DESIGNATION OF DATA PRIVACY OFFICER AND DATA SECURITY OFFICER.

(a) IN GENERAL.—A covered entity shall designate—

(1) 1 or more qualified employees or contractors as data privacy officers; and

(2) 1 or more qualified employees or contractors (in addition to any employee or contractor designated under paragraph (1)) as data security officers.

(b) RESPONSIBILITIES OF DATA PRIVACY OFFICERS AND DATA SECURITY OFFICERS.—An employee or contractor who is designated by a covered entity as a data privacy officer or a data security officer shall be responsible for, at a minimum, coordinating the covered entity's policies and practices regarding—

(1) in the case of a data privacy officer, compliance with the privacy requirements with respect to covered data under this Act; and

(2) in the case of a data security officer, the security requirements with respect to covered data under this Act.

SEC. 302. INTERNAL CONTROLS.

A covered entity shall maintain internal controls and reporting structures to ensure that appropriate senior management officials of the covered entity are involved in assessing risks and making decisions that implicate compliance with this Act.

SEC. 303. WHISTLEBLOWER PROTECTIONS.

(a) DEFINITIONS.—For purposes of this section:

(1) WHISTLEBLOWER.—The term ''whistleblower'' means any employee or contractor of a covered entity who voluntarily provides to the Commission original information relating to non-compliance with, or any violation or alleged violation of, this Act or any regulation promulgated under this Act.

(2) ORIGINAL INFORMATION.—The term ''original information'' means information that is provided to the Commission by an individual and—

(A) is derived from the independent knowledge or analysis of an individual;

(B) is not known to the Commission from any other source at the time the individual provides the information; and

(C) is not exclusively derived from an allegation made in a judicial or an administrative action, in a governmental report, a hearing, an audit, or an investigation, or from news media, unless the individual is a source of the allegation.

(b) EFFECT OF WHISTLEBLOWER RETALIATIONS ON PENALTIES.—In seeking penalties under section 401 for a violation of this Act or a regulation promulgated under this Act by a covered entity, the Commission shall consider whether the covered entity retaliated against an individual who was a whistleblower with respect to original information that led to the successful resolution of an administrative or judicial action brought by the Commission or the Attorney General of the United States under this Act against such covered entity.

TITLE IV—ENFORCEMENT AUTHORITY AND NEW PROGRAMS

SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation pro-

mulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in paragraphs (3) and (4), the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(C) LIMITING CERTAIN ACTIONS UNRELATED TO THIS ACT; AUTHORITY PRESERVED.—

(i) IN GENERAL.—The Commission shall not bring any action to enforce the prohibition in section 5 of the Federal Trade Commission Act (15 U.S.C. 45) on unfair or deceptive acts or practices with respect to the privacy or security of covered data, unless such action is consistent with this Act.

(ii) RULE OF CONSTRUCTION.—Except as provided in paragraph (1), nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law, or to limit the Commission's authority to bring actions under section 5 of the Federal Trade Commission Act (15 U.S.C. 45) relating to unfair or deceptive acts or practices to enforce the provisions of this Act and regulations promulgated thereunder, including to ensure that privacy policies required under section 102 are truthful and non-misleading.

(3) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of

Attachment #6

the Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner provided in paragraphs (1) and (2) of this subsection, with respect to—

(A) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; and

(B) organizations not organized to carry on business for their own profit or that of their members.

(4) DATA PRIVACY AND SECURITY FUND.—

(A) ESTABLISHMENT OF VICTIMS RELIEF FUND.—There is established in the Treasury of the United States a separate fund to be known as the ''Data Privacy and Security Victims Relief Fund'' (referred to in this paragraph as the ''Victims Relief Fund'').

(B) DEPOSITS.—

(i) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any covered entity in any action the Commission com-

Attachment #6

mences to enforce this Act or a regulation promulgated under this Act.

(ii) DEPOSITS FROM THE ATTORNEY GENERAL.—The Attorney General of the United States shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any covered entity in any action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.

(C) USE OF FUND AMOUNTS.—Amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been imposed under this Act. To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of consumer or business education relating to data privacy and security or for the purpose of engaging in technological research that the Commission considers necessary to enforce this Act.

(D) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Victims Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Commission $100,000,000 to carry out this Act.

(b) ENFORCEMENT OF SECTION 206.—This section shall not apply to a violation of section 206 or a regulation promulgated under such section, and such section shall be enforced under subsection (d) of such section.

SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTION.—Except as provided in subsection (h), in any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(1) enjoin that act or practice;

(2) enforce compliance with this Act or the regulation;

(3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; or

(4) obtain such other relief as the court may consider to be appropriate.

(b) Rights of the Commission.—

(1) In general.—Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—

(A) be heard on all matters arising in such action; and

(B) file petitions for appeal of a decision in such action.

(2) Notification timeline.—Where it is not feasible for the attorney general of a State to provide the notification required by paragraph (2) before initiating a civil action under paragraph (1), the

Attachment #6

attorney general shall notify the Commission immediately after initiating the civil action.

(c) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL.—Whenever a civil action under subsection (a) is pending and another civil action or actions are commenced pursuant to such subsection in a different Federal district court or courts that involve 1 or more common questions of fact, such action or actions shall be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia; provided however, that no such action shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by the attorney general of the State.

(d) ACTIONS BY COMMISSION.—In any case in which a civil action is instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act, no attorney general of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act that is alleged in such complaint.

(e) INVESTIGATORY POWERS.—Nothing in this section shall be construed to prevent the attorney general of a State or another authorized official of a State from exercising the powers conferred on the attorney general or the State official by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(f) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(g) ACTIONS BY OTHER STATE OFFICIALS.—

(1) IN GENERAL.—Any State official who is authorized by the State attorney general to be the exclusive authority in that State to enforce this Act may bring a civil action under subsection (a), subject to the same requirements and limitations that

Attachment #6

apply under this section to civil actions brought under such subsection by State attorneys general.

(2) AUTHORITY PRESERVED.—Nothing in this section shall be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(h) EXCLUSION OF SECTION 206.—This section shall not apply to a violation of section 206 or a regulation promulgated under such section.

SEC. 403. AUTHORITY OF COMMISSION TO SEEK PERMANENT INJUNCTION AND OTHER EQUITABLE REMEDIES.

(a) IN GENERAL.—Section 13 of the Federal Trade Commission Act (15 U.S.C. 53) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking ‘‘is violating, or is about to violate,’’ and inserting ‘‘has violated, is violating, or is about to violate’’;

(B) in paragraph (2)—

(i) by inserting ‘‘either (A)’’ before ‘‘the enjoining thereof’’; and

(ii) by inserting ‘‘or (B) the permanent enjoining thereof or the ordering of

Attachment #6

an equitable remedy under subsection (e)'' after ''final,''; and

(C) in the flush text following paragraph (2)—

(i) by striking ''to enjoin any such act or practice'' and inserting ''to obtain such injunction or remedy'';

(ii) by striking ''Upon a proper showing that'' and inserting ''In a case brought under paragraph (2)(A), upon a proper showing that'';

(iii) by striking ''such action'' and inserting ''a temporary restraining order or preliminary injunction'';

(iv) by striking ''without bond'';

(v) by striking ''That in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction.'' and inserting the following: ''That in a case brought under paragraph (2)(B), after proper proof and upon a showing that a permanent injunction or equitable remedy under subsection (e) would be in the public interest, the court may issue a permanent injunction, an equitable remedy under subsection (e), or any other relief as the court determines to be just and proper, including temporary or preliminary equitable relief.'';

(vi) by inserting ''under paragraph (2)'' after ''Any suit''; and

(vii) by striking ''any suit under this section'' and inserting ''any such suit''; and

(2) by adding at the end the following new subsection:

''(e) EQUITABLE REMEDIES.—

''(1) RESTITUTION; CONTRACT RESCISSION AND REFORMATION.—

''(A) IN GENERAL.—In a suit brought under subsection (b)(2)(B) with respect to a violation of a provision of law enforced by the Commission, the Commission may seek, and the court may order—

''(i) restitution for consumer loss resulting from such violation;

''(ii) rescission or reformation of contracts; and

''(iii) the refund of money or return of property.

Attachment #6

"(B) LIMITATIONS PERIOD.—Relief under this paragraph shall not be available for a claim arising more than 10 years before the filing of the Commission's suit under subsection (b)(2)(B) with respect to the violation that gave rise to the claim.

"(2) DISGORGEMENT.—

"(A) IN GENERAL.—In a suit brought under subsection (b)(2)(B) with respect to a violation of a provision of law enforced by the Commission, the Commission may seek, and the court may order, disgorgement of any unjust enrichment that a person obtained as a result of that violation.

"(B) CALCULATION.—Any disgorgement that is ordered with respect to a person under subparagraph (A) shall be offset by any amount of restitution that the person is ordered to pay under paragraph (1).

"(C) LIMITATIONS PERIOD.—Disgorgement under this paragraph shall be limited to any unjust enrichment a person, partnership, or corporation obtained in the 10 years preceding the filing of the Commission's suit under subsection (b)(2)(B) with respect to the violation that resulted in such unjust enrichment.

"(3) CALCULATION OF LIMITATIONS PERIODS.—For purposes of calculating any limitations period with respect to a claim for relief under paragraph (1) or a disgorgement order under paragraph (2), any time in which a person, partnership, or corporation against which such relief or order is sought is outside the United States shall not be counted for purposes of calculating such period.".

(b) CONFORMING AMENDMENTS.—Section 16(a)(2) of the Federal Trade Commission Act (15 U.S.C. 56(a)(2)) is amended—

(1) in subparagraph (A), by striking "(relating to injunctive relief)"; and

(2) in subparagraph (B), by striking "(relating to consumer redress)".

(c) APPLICABILITY.—The amendments made by this section shall apply with respect to any action or proceeding that is commenced on or after the date of enactment of this Act.

SEC. 404. APPROVED CERTIFICATION PROGRAMS.

(a) IN GENERAL.—The Commission shall establish a program in which the Commission shall approve voluntary consensus standards or certification programs that cov-

Attachment #6

ered entities may use to comply with 1 or more provisions in this Act.

(b) EFFECT OF APPROVAL.—A covered entity in compliance with a voluntary consensus standard approved by the Commission shall be deemed to be in compliance with the provisions of this Act.

(c) TIME FOR APPROVAL.—The Commission shall issue a decision regarding the approval of a proposed voluntary consensus standard not later than 180 days after a request for approval is submitted.

(d) EFFECT OF NON-COMPLIANCE.—A covered entity that claims compliance with an approved voluntary consensus standard and is found not to be in compliance with such program by the Commission or in any judicial proceeding shall be considered to be in violation of the section 5 of the Federal Trade Commission Act (15 U.S.C. 45) prohibition on unfair or deceptive acts or practices.

(e) RULEMAKING.—Not later than 120 days after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing a process for review of requests for approval of proposed voluntary consensus standards under this section.

(f) REQUIREMENTS.—To be eligible for approval by the Commission, a voluntary consensus standard shall meet the requirements for voluntary consensus standards set forth in Office of Management and Budget Circular A–119, or other equivalent guidance document, ensuring that they are the result of due process procedures and appropriately balance the interests of all the stakeholders, including individuals, businesses, organizations, and other entities making lawful uses of the covered data covered by the standard, and—

(1) specify clear and enforceable requirements for covered entities participating in the program that provide an overall level of data privacy or data security protection that is equivalent to or greater than that provided in the relevant provisions in this Act;

(2) require each participating covered entity to post in a prominent place a clear and conspicuous public attestation of compliance and a link to the website described in paragraph (4);

(3) include a process for an independent assessment of a participating covered entity's compliance with the voluntary consensus standard or certification program prior to certification and at reasonable intervals thereafter;

(4) create a website describing the voluntary consensus standard or certification program's goals and requirements, listing participating covered enti-

ties, and providing a method for individuals to ask questions and file complaints about the program or any participating covered entity;

(5) take meaningful action for non-compliance with the relevant provisions of this Act by any participating covered entity, which shall depend on the severity of the non-compliance and may include—

(A) removing the covered entity from the program;

(B) referring the covered entity to the Commission or other appropriate Federal or State agencies for enforcement;

(C) publicly reporting the disciplinary action taken with respect to the covered entity;

(D) providing redress to individuals harmed by the non-compliance;

(E) making voluntary payments to the United States Treasury; and

(F) taking any other action or actions to ensure the compliance of the covered entity with respect to the relevant provisions of this Act; and

(6) issue annual reports to the Commission and to the public detailing the activities of the program and its effectiveness during the preceding year in en-

suring compliance with the relevant provisions of this Act by participating covered entities and taking meaningful disciplinary action for non-compliance with such provisions by such entities.

SEC. 405. RELATIONSHIP BETWEEN FEDERAL AND STATE LAW.

(a) RELATIONSHIP TO STATE LAW.—No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or data security and associated activities of covered entities.

(b) SAVINGS PROVISION.—Subsection (a) may not be construed to preempt State laws that directly establish requirements for the notification of consumers in the event of a data breach.

(c) RELATIONSHIP TO OTHER FEDERAL LAWS.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), the requirements of this Act shall supersede any other Federal law or regulation relating to the privacy or security of covered data or associated activities of covered entities.

(2) SAVINGS PROVISION.—This Act may not be construed to modify, limit, or supersede the operation of the following:

(A) The Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

(B) The Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(C) Section 227 of the Communications Act of 1934 (47 U.S.C. 227).

(D) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq).

(E) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(F) The Health Insurance Portability and Accountability Act (Public Law 104–191).

(G) The Electronic Communications Privacy Act (18 U.S.C. 2510 et seq.).

(H) Section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly referred to as the ''Family Educational Rights and Privacy Act of 1974'').

(I) The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq).

(J) The Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.).

(K) The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq).

Attachment #6

(3) COMPLIANCE WITH SAVED FEDERAL LAWS.—To the extent that the data collection, processing, or transfer activities of a covered entity are subject to a law listed in paragraph (2), such activities of such entity shall not be subject to the requirements of this Act.

(4) NONAPPLICATION OF FCC LAWS AND REGULATIONS TO COVERED ENTITIES.—Notwithstanding any other provision of law, neither any provision of the Communications Act of 1934 (47 U.S.C. 151 et. seq.) and all Acts amendatory thereof and supplementary thereto nor any regulation promulgated by the Federal Communications Commission under such Acts shall apply to any covered entity with respect to the collection, use, processing, transferring, or security of individual information, except to the extent that such provision or regulation pertains solely to "911" lines or other emergency line of a hospital, medical provider or service office, health care facility, poison control center, fire protection agency, or law enforcement agency.

SEC. 406. CONSTITUTIONAL AVOIDANCE.

The provisions of this Act shall be construed, to the greatest extent possible, to avoid conflicting with the Constitution of the United States, including the protections

Attachment #6

of free speech and freedom of the press established under the First Amendment to the Constitution of the United States.

SEC. 407. SEVERABILITY.

If any provision of this Act, or an amendment made by this Act, is determined to be unenforceable or invalid, the remaining provisions of this Act and the amendments made by this Act shall not be affected.

Attachment #7

Client Alert

Bill to Expand Medical Data Exemptions and Harmonize HIPAA and CA De-Identification is APPROVED by the CA Legislature

Quick Summary

CA AB 713 has been approved by the CA legislature. The bill is now headed to Governor Newsom's desk, awaiting his signature or veto by September 30, 2020.

This legislation marks a remarkable step forward for healthcare providers and medical research—and for patients. The bill will lessen burdens that the 2018 California Consumer Privacy Act (CCPA) imposed on medical research and healthcare operations by harmonizing the CCPA with federal law. Specifically, the bill will:

- Exempt from the CCPA medical research data that is already tightly regulated by federal regulations;
- Harmonize the CA definition of de-identified patient data with the existing federal definition of de-identification; and
- Make CCPA exemptions for HIPAA Business Associates parallel to those for HIPAA Covered Entities.

The bill also establishes new privacy protections regarding de-identified patient data. The bill will:

- Require new contractual safeguards if de-identified patient data is sold;
- Impose new notice requirements regarding the sale of de-identified patient data; and
- Create a first-in-the-nation ban on the re-identification of de-identified patient data.

CA AB 713 reflects an extraordinary consensus reached by privacy advocates and healthcare providers, medical research organizations, and life science companies. If enacted, it will take effect immediately.

WALDO LAW OFFICES PLLC

September 14, 2020

Attachment #7

Background – The Problem CA AB 713 is Intended to Address

The CCPA, which took effect on January 1, 2020, contains provisions considered to be problematic and confusing for healthcare and life sciences companies and burdensome to medical research. Among the concerns are that:

(a) The CCPA's exemption for medical research is too narrow, because it only exempts clinical trial data, which comprises only a small swath of all clinical research data;
(b) The CCPA has a CA-unique definition of "deidentified"[1] data exempt from the law, which is not based on or harmonized with the HIPAA definition of de-identified data that has long been foundational in health data research; and
(c) The exemptions for HIPAA Covered Entities (essentially, providers and plans) and for HIPAA Business Associates (essentially, their vendors who access Protected Health Information, or PHI) are not parallel, which poses compliance questions for certain Business Associates.

1.1.2020 – CCPA takes effect

1.8.2020 – CA AB 713 to address health data concerns passes Senate Health. Supportive testimony from ACRO and AdvaMed

8.31.2020 – AB 713 passes Senate, 37-0

9.1.2020 – Assembly concurs, 77-0

9.30.2020 – Deadline for Governor to sign or veto

If signed, AB 713 takes effect immediately

The Legislative Process

Since 2019, a coalition of healthcare and life science organizations has been advocating to reduce the CCPA's burdens on research and healthcare. Led by AdvaMed, with legal support from Waldo Law Offices, the group worked closely with a coalition of privacy groups supportive of the CCPA. The privacy groups supported alleviating the CCPA's unintentional burdens on medical research, but only if key CCPA protections were not undermined. It is a remarkable—and encouraging—part of the bill's story that the health coalition and the privacy coalition together achieved an extraordinary consensus, based on a shared commitment to protect both patient privacy and medical research.

To address the concerns about research and healthcare, Assemblyman Kevin Mullin put legislative "fix" language into CA AB 713 in early January 2020. The Senate Health Committee held a hearing in which Doug Peddicord of the Association of Clinical Research Organizations (ACRO) and Fielding Greaves of AdvaMed testified in support. Numerous others also voiced support, and the bill was reported out unanimously. Over the next months, legislative staff and stakeholders continued to discuss the bill's details. It was amended and reported out by the Senate Appropriations Committee. On August 31, the bill came to the Senate floor and was passed unanimously. The Assembly concurred unanimously with the Senate changes. The bill now awaits the Governor Newsom's signature or veto. Because

[1] HIPAA refers to "de-identified" data, while the CCPA refers to "deidentified" data. For convenience, the HIPAA spelling is used in this Alert.

the bill contains an urgency clause and was approved by more than a 2/3 vote in each chamber, it will take effect immediately if enacted.

The Bill's Provisions

(1) Harmonization of De-Identification for Health Data

Under federal law, data that has been de-identified in accordance with HIPAA's regulatory standard (found here) is no longer subject to HIPAA. Under the CCPA, data that has been de-identified in accordance with the CCPA definition (found here) is no longer subject to the CCPA. Because HIPAA and the CCPA have different standards for de-identifying information, documenting that specified data sets meet both HIPAA and CCPA standards can result in uncertainty, delays, and legal costs, all of which is likely to compromise medical research.

AB 713 addresses that inconsistency by providing that data is exempt from the CCPA if both of the following are true:

- The data is de-identified in accordance with HIPAA, and
- The data is derived from patient information originally governed by HIPAA, the California Confidentiality of Medical Information Act (CMIA), or the federal Common Rule applicable to federally funded research. As newly defined in AB 713, "patient information," includes PHI and individually identifiable health information, as defined by HIPAA; Medical Information, as defined by the CMIA; or identifiable private information, as defined by the Common Rule.

The bill further provides that if patient data that had been HIPAA de-identified were to later become re-identified, the data would become subject to applicable federal and state privacy laws. *See* CA Civil Code section 1798.146(a)(4).

(2) Broadening of Research Data Exemption

Existing law exempts from the CCPA only clinical trial data—specifically, information collected as part of a clinical trial subject to the Common Rule, pursuant to Good Clinical Practice guidelines, or pursuant to FDA human subject protection requirements.

CA AB 713 exempts research data more broadly. The exemption covers information collected, used, or disclosed in research that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of HIPAA, the Common Rule, Good Clinical Practice Guidelines, or FDA human subject protections. *See* CA Civil Code section 1798.146(a)(5). This is important because much research happens outside of "clinical trials," such as the use of clinical data from electronic health records to study drug and vaccine safety. A "clinical trial" includes only interventional research that tests a new drug, device, or biologic.

(3) Clarification of Business Associate Exemption

Under existing law, PHI under HIPAA and Medical Information under the CMIA are exempt from the CCPA. HIPAA Covered Entities and other healthcare providers are also exempt from the CCPA to the extent they maintain patient information in the same manner as PHI or Medical Information. But the Business Associates exemption is narrower than that for Covered Entities. Business Associates are not exempt with regard to patient information maintained in the same manner as PHI or Medical Information. This raises questions for Business Associates that maintain both PHI and non-PHI patient information together, subject to the same data governance processes and security controls.

AB 713 exempts Business Associates governed by HIPAA from the CCPA to the extent that they maintain, use, and disclose patient information (defined above) in the same manner as PHI or Medical Information. *See* CA Civil Code section 1798.146(a)(3).

(4) Ban on Re-Identification of De-Identified Patient Data

AB 713 creates a first-in-the-US ban on the re-identification of previously de-identified health data, subject to certain exceptions.

"Re-identification" is defined as the process of reversing de-identification, by adding specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual, or the use of any statistical method, contrivance, computer software, or other means that have the effect of associating de-identified information with a specific identifiable individual.

The exceptions to the ban allow re-identification:

(a) For Treatment, Payment, or Healthcare Operations, as defined by HIPAA;
(b) For public health activities or purposes described in HIPAA here;
(c) For research conducted in accordance with HIPAA or the Common Rule;
(d) Pursuant to a contract where the lawful holder of the de-identified patient information expressly engages someone to attempt to re-identify the de-identified information in order to conduct testing, analysis, or validation of de-identification, or related statistical techniques, if the contract bans any other use or disclosure of the re-identified data and requires that it be returned or destroyed upon contract termination; or
(e) If required by law.

Any re-identified patient information (even where re-identification was permissible under one of the exceptions above) becomes subject to applicable federal and state privacy and security laws. *See* CA Civil Code section 1798.148(a)-(b).

(5) Contract Requirements for the Sale of De-Identified Health Data

Beginning January 1, 2021, new contractual terms must be included in any contract for the sale or license of de-identified patient information where one of the parties is a California resident or does business in California. Such contracts must include the following, or substantially similar, terms:

(a) A statement that the de-identified information being sold or licensed includes de-identified patient information;
(b) A statement that re-identification and attempted re-identification by the purchaser or licensor is prohibited by CA Civil Code sec. 1798.148; and
(c) A requirement that, unless otherwise required by law, the purchaser or buyer may not further disclose the de-identified information unless the recipient is contractually bound by the same or stricter restrictions and conditions.

See CA Civil Code section 1798.148(c).

(6) Notice Requirements Regarding Sale of De-Identified Data

For businesses that sell or disclose HIPAA-de-identified data derived from patient information (which is exempt from the CCPA because it falls within the newly harmonized definition), the bill imposes new notice requirements. Such businesses must include in their privacy policy whether the business sells or discloses de-identified data that was derived from patient information and if so, whether that patient information was de-identified pursuant to one or more of the permissible HIPAA de-identification methods—*i.e.*, the HIPAA Safe Harbor or expert determination method. *See* CA Civil Code section 1798.130.

Legal Stance of AB 713 Provisions in Light of Proposition 24/CPRA

Proposition 24, a ballot initiative on the ballot this November, would enact the California Privacy Rights and Enforcement Act (CPRA), which, if enacted, would replace the CCPA. The legislature could amend the CPRA only to "enhance privacy and . . . [adopt measures] that are consistent with and further the purposes and intent of the Act."

Supporters of AB 713 have been concerned that if the legislature enacted the bill prior to November, and then voters approved the CPRA in November, the CPRA would supersede and nullify the changes made by AB 713. Accordingly, to prevent that outcome, Assemblyman Kevin Mullin recently amended AB 713 to create new code sections to house the new provisions beneficial to research and healthcare described above. These provisions are in new CA Civil Code sections 1798.146 and 1798.148. Those sections do not exist in current law, nor do they exist in the CPRA. By creating new code sections, the bill's author and supporters intend to ensure that these broadened health-related exemptions, as well as the bill's ban on re-identification of de-identified data, endure despite possible enactment of the CPRA.

Attachment #7

Supporters of the Bill

The following organizations endorsed the bill. As noted earlier, privacy groups were also closely involved and contributed to the bill. Supporters were:

Advanced Medical Technology Association
Association of Clinical Research Organizations
Association of Regional Center Agencies
Biocom
Biotechnology Innovation Organization
California Association of Health Plans
California Biomedical Research Association
California Dental Association
California Hospital Association
California Life Sciences Association
California Retailers Association
Consumer Healthcare Products Association
International Pharmaceutical & Medical Device Privacy Consortium
Medical Imaging and Technology Alliance
National Association of Chain Drug Stores
Pharmaceutical Research and Manufacturers of America

Attachment #8

Diane Sacks LLC

August 10, 2020

Privacy and Security Round Up

Capital One Fine $80 million for 2019 Data Breach

On August 6, 2020, the Office of the Comptroller of the Currency (OCC) announced that it had imposed a civil monetary penalty of $80 million on Capital One in connection with a 2019 data breach that compromised the personal information of about 106 million customers. In its Consent Order, the OCC found that Capital One had failed to implement risk assessment processes or establish appropriate risk management, such as adequate network and data loss prevent controls, for the cloud environment. It also faulted the bank's internal audit for failing to identify "numerous control weaknesses and gaps" in the cloud environment, and its board for failing to take effective actions to hold management accountable for addressing those gaps that were raised by internal audit.

Comments: In announcing the penalty, the OCC noted that it had "positively considered the bank's customer notification and remediation efforts." This was likely one reason the Capital One fine is considerably lower than the $700 million paid by Equifax in its settlement with the Federal Trade Commission (FTC) and 50 states for a 2017 hack affecting the personal data of approximately 147 million consumers, and for which Equifax was faulted for delaying 6 weeks before notifying consumers.

Final Rule on the Confidentiality of Substance Use Disorder (SUD) Patient Records

On July 15, 2020, the Department of Health and Services published a final rule easing some of the restrictions on the use and disclosure of SUD patient records governed by 42 CFR Part 2 (Part 2 records). The Department of Health and Human Services (HHS) issued a Fact Sheet summarizing the changes made by the rule, including clarifying that Part 2 records do not include records about a SUD patient created by non-Part 2 providers, allowing written consent for the disclosure of Part 2 records for any payment and health care operation purposes, including care coordination and case management, and allowing disclosure of Part 2 records for research purposes to non-HIPAA entities under the same conditions as permitted by HIPAA.

Comments: While the rule narrows the application of Part 2 and reduces the burdens associated with sharing Part 2 data, the changes are incremental, consistent with HHS' existing authority. HHS notes that the rule is intended to be an "interim and transitional step" until it issues a regulation to implement the changes to Part 2 required by the CARES Act. Once issued, that new regulation should bring Part 2 into much closer alignment with HIPAA, although as noted by HHS in the preamble to this rule, it may not take effect before March 27, 2021.

US and EU Respond to Schrems II Decision

In the wake of the July 16, 2020 decision (known as "Schrems II") by the Court of Justice of the European Union (CJEU) declaring the EU-U.S. Privacy Shield as an invalid mechanism for transferring personal data from the European Union to the United States, the U.S. Department of Commerce and the European Commission issued a joint statement on August 10, 2020 that they have initiated discussions to evaluate the potential for an "enhanced EU-U.S. Privacy Shield framework" that will comply with the Schrems II decision.

Comments: Given the importance of the continued flow of data between the EU and US and the limitations of standard contract clauses for this purpose, it is not surprising that the US and EU are acting quickly to find a mechanism to replace the Privacy Shield Framework. However, it will be a daunting endeavor without a change in US surveillance laws, which were the basis for the unravelling not only of the Privacy Shield Framework by Schrems II, but also of the previous Safe Harbor Framework in the first Schrems decision in 2015.

Attachment #8

FCC Investigates Monetization of "Bidstream" Data

On August 5, 2020 the Federal Communications Commission (FCC) announced that it had sent letters to AT&T and Verizon inquiring about the aggregation and monetization of consumer location and other personal data that is generated when companies engage in real-time bidding (RTB) for advertising placement purposes (so-called "bidstream data"). The FCC cites media reports that the data is being used to track locations to protests and places of worship, and follows a letter sent by a bipartisan group of members of Congress to the FTC requesting an investigation into these practices.

Comments: The letter by members of Congress states that the identity of the companies selling the bidstream data to data brokers remains unknown. However, the FCC appears to believe that internet service providers (ISPs), such as AT&T and Verizon, are at least partially responsible in that it asks them to explain how these practices are not the "functional equivalent" of practices they had told the FCC that they had discontinued, namely, the sale of consumer location data. It comes little more than a month after a US District Court denied a preliminary challenge by ISPs to a 2019 Maine law that requires ISPs to obtain consumer consent before using, distributing or selling their personal information.

Federal Biometric Data Protection Bill Introduced

On August 4, 2020, Senators Merkley (D-OR) and Sanders (I-VT) introduced a federal biometrics bill that would require private entities to obtain written consent to collect or disclose an individual's biometric data, and would prohibit the sale or disclosure of such data for profit. Private entities in possession of biometric data would be required to develop a public written policy that establishes a retention schedule and guidelines for permanently destroying biometric information in their possession. The bill provides for a private right of action and states that a violation of its provisions constitutes "an injury-in-fact and a harm to any affected individual." The bill would not apply to data collected for treatment, payment or health care operations under HIPAA.

Comments: This bill follows other recent federal bills that would limit or prohibit the use of biometric data although, unlike some of the other bills, it focuses on private entities' rather than the government's use of such data. Its private right of action appears to draw on the Illinois Biometric Information Protection Act, which has resulted in employers facing a multitude of class action lawsuits.

Lifespan Agrees to Pay $1,040,000 to OCR for HIPAA Violations Related to an Unencrypted Laptop

On July 27, 2020, the HHS Office of Civil Rights (OCR) announced a settlement with Lifespan Health System arising out of an April 2017 breach report to OCR by Lifespan Corporation, the parent company of Lifespan. The breach involved the theft of an unencrypted laptop containing the protected health information (PHI) of over 20,000 individuals. OCR found there was "systematic noncompliance" with HIPAA, including the failure to encrypt PHI on laptops after Lifespan determined it should do so, a lack of device and media controls, and the lack of a business associate agreement between the Lifespan affiliated covered entity and its parent corporation.

Comments: As is often the case, the OCR investigation and settlement in this case was triggered by a breach notification, and the cause of the breach was a mixture of both technical and non-technical missteps. Some of these could have been addressed by better processes, such as policies for encrypting portable media and identifying business associate relationships, and others by better security training and awareness, which might have led the employee in question to not leave the laptop in a car in a public lot.

Please contact Diane Sacks at dsacks@sacksllc.com or (202)459-2101 for more information on any of these items. This newsletter is intended to provide general information only and is not intended as legal advice.

Attachment #9

Trust, but Verify:
Informational Challenges Surrounding AI-Enabled Clinical Decision Software

The CENTER for INNOVATION POLICY at DUKE LAW

Duke
MARGOLIS CENTER
for Health Policy

Attachment #9

Authors

Christina Silcox, Managing Associate, Duke-Margolis Center for Health Policy

Arti Rai, Elvin R. Latty Professor of Law and Co-Director, The Center for Innovation Policy, Duke University School of Law

Isha Sharma, Senior Research Assistant, Duke-Margolis Center for Health Policy

Acknowledgements

The authors would like to deeply thank many people for contributing their time and expertise to inform and improve this white paper. The paper would not have been possible without the input of expert perspectives from a May 2019 private workshop and January 2020 public meeting, both held in Washington, DC. Additionally, the Duke team held many informational meetings and calls with various stakeholders across the artificial intelligence and health care ecosystem over the course of this project. We are extremely grateful for their time and thoughtful feedback on working drafts.

We would also like to thank Patricia Green, the Duke-Margolis Center's Director of Communications, for her editorial support and Kerry Stenke from the Duke Clinical Research Institute for her support in developing graphics for this white paper. Finally, we would like to thank Duke University's Balfour Smith, Bennett Wright, Michael McCarthy, and Nikhil Gadiraju for their contributions to the research and editing of this report.

Funding

This publication was funded by the Greenwall Foundation.

Disclosures

Any opinions expressed in this paper are solely of those of the authors and do not represent the views or policies of other organizations external to Duke.

Attachment #9

About the Duke-Margolis Center for Health Policy

The Robert J. Margolis, MD, Center for Health Policy at Duke University is directed by Mark McClellan, MD, PhD, and brings together expertise from Washington, DC, the broader policy community, Duke University, and Duke Health to address the most pressing issues in health policy. The mission of the Duke-Margolis Center is to improve health and the value of health care through practical, innovative, and evidence-based policy solutions. Duke-Margolis catalyzes Duke University's leading capabilities, including interdisciplinary academic research and capacity for education and engagement to inform policy-making and implementation for better health and health care. For more information, visit healthpolicy.duke.edu.

About the Center for Innovation Policy at Duke Law

The Center for Innovation Policy at Duke Law (CIP), led by Faculty Co-Directors Arti Rai and Stuart Benjamin, is a forum for independent analysis of policies for promoting technological innovation that enhances long-term social welfare. CIP brings together technology and business leaders, government officials, lawyers, and academics to identify improvements in legal frameworks and policies that directly affect innovation. These include intellectual property, other R&D incentives, as well as industry-specific regulation in life sciences, information, and communications. CIP draws on the expertise of affiliated faculty across the University. A board of distinguished business leaders and former public officials advises the Center's leadership. For more information, visit law.duke.edu/innovationpolicy.

Introduction

From improving diagnosis and personalizing treatment decisions, to determining how best to meet the needs of underserved populations, artificial intelligence (AI) systems have the potential to revolutionize health care.[1] By 2021, the size of the health AI market will be about 11 times what it was in 2014, growing from $600 million to an estimated $6.6 billion.[2] This field is complex, and as with all technologies, not without risk. As such, it is important for manufacturers of AI-enabled software products to communicate information to clinicians, health system operators, and others about how to harness the benefits of AI while reducing risk.

AI refers to the ability of a machine to perform a task normally done by humans. AI-enabled clinical decision software is software that assists or automates the task of clinical decision-making around risk assessment, diagnosis, and treatment. AI-enabled software can be classified into two categories: rules-based and data-based algorithms. Rules-based algorithms use expert-derived rules and defined and logical processes to turn multiple inputs into an output—for example, an alert that reminds a physician that their patient is due for their colonoscopy based on clinically-accepted schedule guidelines. By contrast, data-based algorithms[*] are given sets of labeled input data (called "training data") and use programmed processes to derive relationships between the inputs and the so-called "labels"—for instance, labels that classify thousands of mammograms by whether or not the patient was eventually diagnosed with cancer. The derived relationships can then be used to predict how new input data is likely to be labeled. This paper will focus on data-based learning that uses labeled training data. This type of learning is generally called supervised learning (see **Figure 1**).

For years, providers have used rules-based AI in clinical decision software[†] to help make diagnoses and treatment decisions, manage population health, and carry out general administrative duties. However, recent advances in machine learning can improve the performance of software by opening the door to a range of new AI-enabled software that can guide more complex decision-making.

For logistical, technical, legal, or competitive reasons, manufacturers of AI-enabled tools, particularly data-based AI tools, might not disclose information about design, materials, and mechanism of action[‡] to regulators, purchasers, and users. Additionally, business considerations play a role in limiting disclosure. For-profit firms protect innovation through a variety of mechanisms, including patents and trade secrecy.[§] Incentives to keep training datasets proprietary may be reinforced by concerns about compliance with data privacy protections or security requirements. But risk assessment, and ultimately adoption, may be complicated if manufacturers or developers are reluctant to disclose trade secrets.

[*] Data-based AI is often referred to as "machine learning."

[†] This paper purposely uses a broad term *clinical decision software* to be inclusive of clinical decision support (CDS) software that is not under FDA authority, device CDS, and other Software as a Medical Device (SaMD) that goes beyond supporting a clinician in their decision-making by driving or automating the next medical intervention.

[‡] This white paper defines the term *mechanism of action* as a proven physiological explanation of how a medical product produces a therapeutic effect on a living organism or in a biochemical system.

[§] In addition to patents and trade secrecy, trademark law can play a role in protecting businesses against competitors that falsely claim that a given piece of software was developed by their firm. This paper does not address trademark law, as that law protects integrity of information about the *source* of a product, not information about how the product works.

This is because concerns around liability can be expected to influence health systems' evaluation of the associated benefits and risks of implementation and use.

Building and Testing Supervised Machine Learning Systems

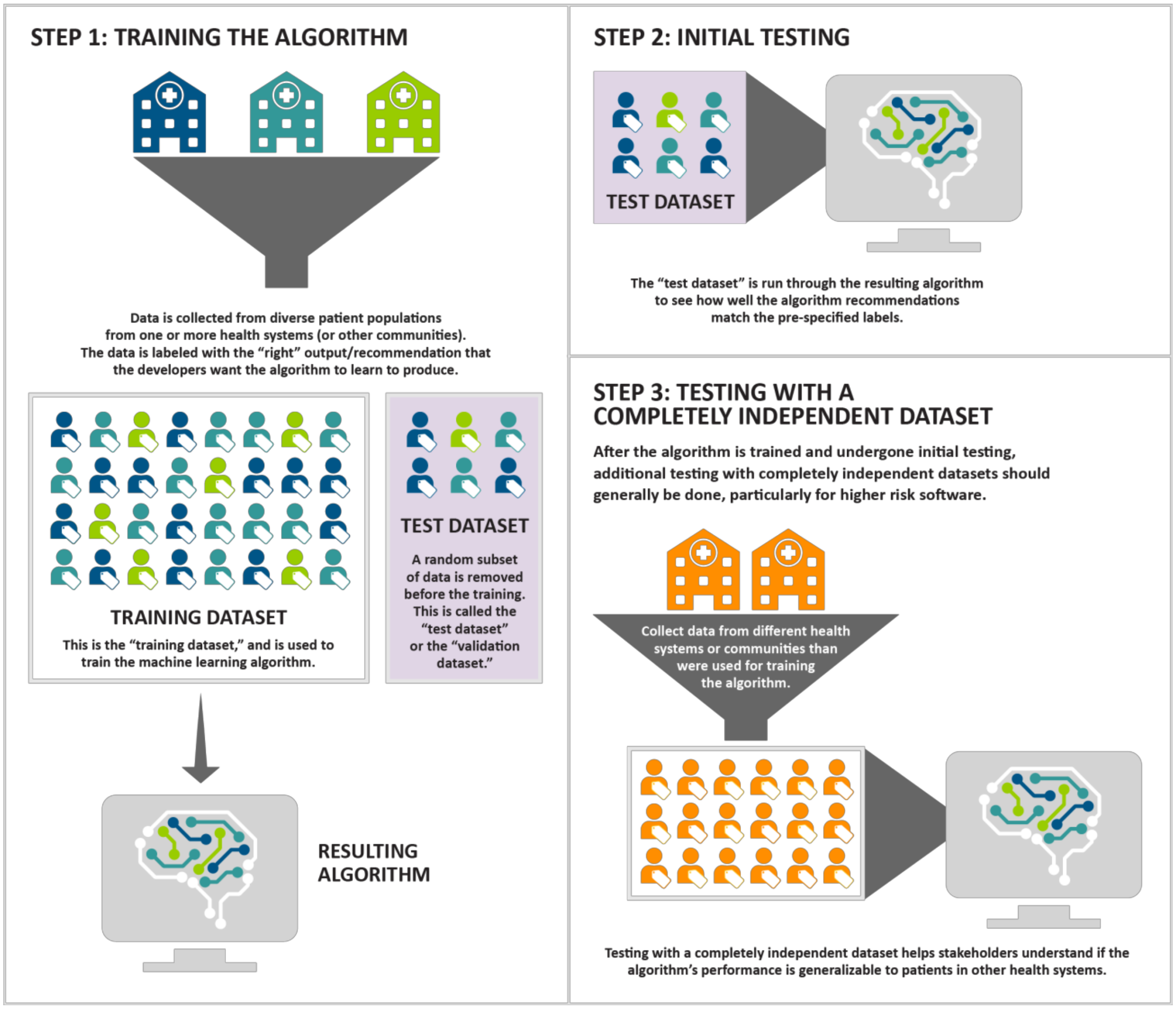

STEP 1: TRAINING THE ALGORITHM
Data is collected from diverse patient populations from one or more health systems (or other communities). The data is labeled with the "right" output/recommendation that the developers want the algorithm to learn to produce.
TRAINING DATASET
This is the "training dataset," and is used to train the machine learning algorithm.
TEST DATASET
A random subset of data is removed before the training. This is called the "test dataset" or the "validation dataset."
RESULTING ALGORITHM
STEP 2: INITIAL TESTING
TEST DATASET
The "test dataset" is run through the resulting algorithm to see how well the algorithm recommendations match the pre-specified labels.
STEP 3: TESTING WITH A COMPLETELY INDEPENDENT DATASET
After the algorithm is trained and undergone initial testing, additional testing with completely independent datasets should generally be done, particularly for higher risk software.
Collect data from different health systems or communities than were used for training the algorithm.
Testing with a completely independent dataset helps stakeholders understand if the algorithm's performance is generalizable to patients in other health systems.

Figure 1. Building and testing supervised machine learning systems. These steps will be discussed in more detail starting on page 7.

This report explores how, in cases where certain information cannot be shared, alternative information could be used to satisfy stakeholder needs. The report is meant to serve as a resource for developers, regulators, clinicians, policy makers, and other stakeholders as they strive to develop, evaluate, adopt, and use AI-enabled medical products. We offer insight into how to incentivize innovation of safe and effective products while communicating information on how and when to use these products. Specific themes include the:

- Ways in which AI-enabled software in health care may differ from traditional medical products;
- Categories of information surrounding AI-enabled clinical software;

- Informational needs and governance structure around AI-enabled clinical software during the total product life cycle; and
- Role of regulatory incentives that protect developer investment, such as patents and trade secrecy, in information flow.

Discussion on informational needs and governance structure is also based on literature review, database searches, perspectives provided during meetings hosted by the Center of Innovation Policy at Duke Law and the Duke-Margolis Center for Health Policy, and individual stakeholder interviews.

What Makes AI-Enabled Clinical Decision Software Different from Other Medical Products?

AI-enabled software differs from traditional medical devices in important ways. These differences create challenges not only for regulators but also for clinicians, health systems, and others who may wish to adopt the technologies. For example, AI-enabled clinical decision software produces clinical recommendations but some of these AI-enabled products might not provide any information as to why and how those recommendations were reached. This lack of information may cause doubts in the minds of clinicians about whether the recommendations or decisions made by the software should be trusted.[3] Lack of trust can be exacerbated by the potential for clinician tort liability if the software recommendation is wrong.[4] Trade secrecy also may limit the amount of information that companies that develop software are willing to disclose, both about how these systems work and how they are built.

This section describes three key differences between AI-enabled software and other medical products: (1) software is powered by health data, which is heterogeneous, complex, and fast-changing; (2) software undergoes more rapid update cycles than other types of medical products; and (3) AI-enabled software might lack an explanation of "how it works."

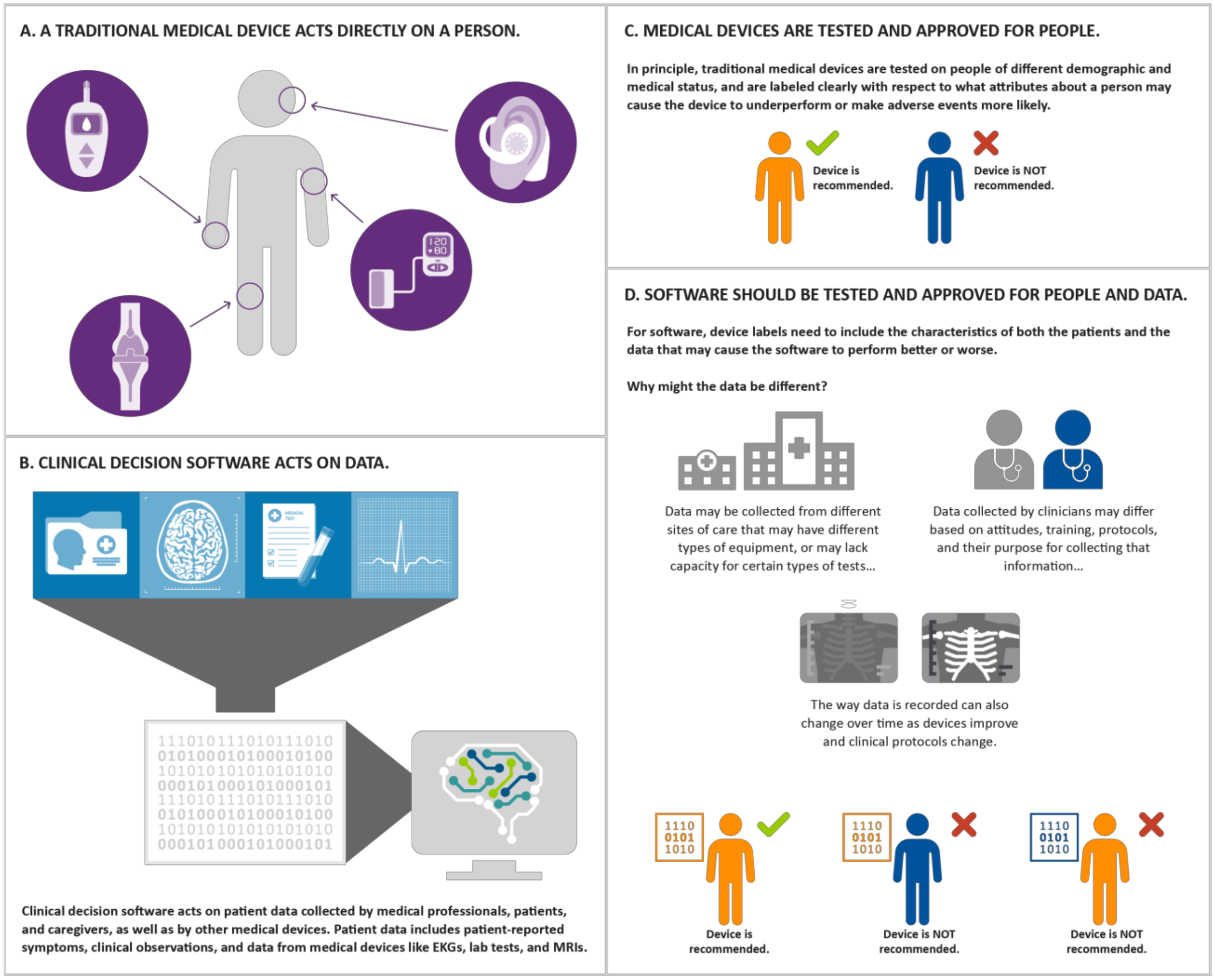
Health Data

Traditional medical devices act on the structure or a sample of the body to produce results (although not through chemical action, which distinguishes devices from drugs). By contrast, software acts on health data which is inputted into the software and analyzed to come to a recommendation or prediction. In addition to acting on health data, machine-learning based software is also built with health data. Health data may consist of data produced through medical imaging, medical sensors such as electrocardiograms, or manually entered in electronic health records (EHRs) or other applications (see **Figure 2**). However, these data can be incomplete, inaccurate, or biased. [5] For example, information gathered from EHRs may be highly disparate in its accuracy and completeness, based on everything from different patients' socioeconomic status and potential language barriers to insurance documentation requirements and system workflows.[6]

Rules-based software produces more consistent output and generally uses limited, structured data elements as inputs. In contrast, data-based software often uses large, complex data sets as inputs; such data are more likely to reflect specific clinical workflows and the perspective of individual physicians, for example through the use of free text fields in EHR records. Patients' access to care, including tests, procedures and insurance coverage, also will affect the amount and types of health data available. Because health data is analyzed by software to reach recommendations, clear definitions around the data input requirements are necessary.

Data-based software manufacturers also use health data to build the algorithms used in their products. Training datasets should be examined to ensure that data is both reliable and relevant, in terms of both the population included and the metadata needed for accuracy and completeness. Due to the heterogeneity discussed above, software developed with data from one location (e.g., a region or hospital) may not work at other locations without significant changes to the software program. Bias can also be a concern. If a software system is not trained with sufficient data that originated from patients from ethnic minorities or patients with co-morbidities, or if the recorded data is historically biased because of socioeconomic status, race, or other criteria, the resulting software may not work well across all populations of patients and may even perpetuate existing biases within the health system.

Software is Powered by Health Data



A. A TRADITIONAL MEDICAL DEVICE ACTS DIRECTLY ON A PERSON.

B. CLINICAL DECISION SOFTWARE ACTS ON DATA.

Clinical decision software acts on patient data collected by medical professionals, patients, and caregivers, as well as by other medical devices. Patient data includes patient-reported symptoms, clinical observations, and data from medical devices like EKGs, lab tests, and MRIs.

C. MEDICAL DEVICES ARE TESTED AND APPROVED FOR PEOPLE.

In principle, traditional medical devices are tested on people of different demographic and medical status, and are labeled clearly with respect to what attributes about a person may cause the device to underperform or make adverse events more likely.

D. SOFTWARE SHOULD BE TESTED AND APPROVED FOR PEOPLE AND DATA.

For software, device labels need to include the characteristics of both the patients and the data that may cause the software to perform better or worse.

Why might the data be different?

Data may be collected from different sites of care that may have different types of equipment, or may lack capacity for certain types of tests...

Data collected by clinicians may differ based on attitudes, training, protocols, and their purpose for collecting that information...

The way data is recorded can also change over time as devices improve and clinical protocols change.

Figure 2. Software is powered by health data.

Accurate labeling of outputs—and the selection of accurate proxies (if proxies are used)—is also important. An October 2019 study described an algorithm that was trained using healthcare expenditures (cost) as a proxy to predict patients' level of risk of serious illness. Even after controlling for potential confounding factors, it was found that white patients use the health care system more than black patients, resulting in higher healthcare expenditures.[7] The algorithm assigned white patients higher risk scores than black patients who were equally ill, thereby reducing the number of black patients who were identified as needing extra care by more than half.[8]

Health data also rapidly changes format and terminology over time as new clinical practices and medical products come into use. Even if these changes result in higher quality data that would improve human decision-making, software may need to be updated to interpret these changes or overall performance can suffer. So, while a well-maintained ultrasound imaging device will perform just as well (or poorly) several years after it is first used, software products designed to analyze ultrasound images may not perform as well when analyzing higher resolution images from a new type of imager or if protocols around the use of contrast agents changes. A software algorithm that uses data such as diagnoses, medication lists, etc., pulled from an EHR will likely degrade in performance over time if it is not updated to account for new medications, treatments, changing standards of care, and the way that these are documented. On the other hand, if (as discussed below) software is updated to reflect changes in underlying data, its performance can improve. As such, manufacturers, health systems and clinicians will need to work together to monitor system performance and update software as needed. The need for software to be regularly updated leads to the next key difference between clinical decision software and traditional medical devices.

Rapid Software Development Cycles

Rapid updating makes software distinctive among medical devices.[9] Manufacturers can act quickly to improve performance and correct problems found through real-world feedback by rapidly pushing updates to the users of those technologies. This is particularly true for AI-enabled software, as certain types of machine learning software have the potential to continuously update themselves in real-time (although it should be noted that clinical decision software of this type has not yet been approved or cleared by the U.S. Food and Drug Administration). These updates are critical to not just improving the product but also maintaining performance.

The rapid development cycle of software is a challenge for regulatory agencies, which have review and clearance processes based on more traditional devices with slower development cycles. The U.S. Food and Drug Administration (FDA) is working to adapt to these differences, including proposing a pre-certification program, which would be a voluntary pathway that would allow manufacturers and FDA to work together to enable rapid innovation and iterative improvements of clinical software while providing appropriate patient safeguards.[10,11] The FDA also released its “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device—Discussion Paper and Request for Feedback” in April 2019,[12] and asked for input from the public regarding how to meet the challenges in regulating the AI-enabled software.

Although frequent product updates should improve performance, they also present concerns for adopters and users of these devices. Best practices need to be developed to clearly inform software users of how updates may impact safe and effective product use. In addition, global updates (i.e., uniform updates sent to all installed software applications) may affect local performance in unexpected ways, emphasizing the need for regular performance monitoring.

Explainability

In the biopharmaceutical arena, certain popular therapies have unknown “mechanisms of action” or “modes of action.”[13,14] This sort of uncertainty is less common with traditional medical devices, though examples exist.[15] Some AI-enabled software products, however, may take uncertainty and its attendant risk—to yet a higher level.

Rules-based software is built on either clear physiological understanding or generally accepted clinical practice guidelines. Clinical practice guidelines may themselves have been built on observed statistical regularities rather than clear mechanism of actions. However, clinical guideline development is a multi-step and generally transparent process involving generating clinical evidence and drawing conclusions that are converted into clinical practice guidelines. Because users can be walked through the inputs and steps used to make the decision, backed up with clinically relevant guidance, rules-based software is generally considered to be “explainable.” In contrast, certain data-based software products may not be able to provide stakeholders with a comprehensible explanation of how they weigh and combine inputs to come to a result, nor relate the recommendations back to physiological explanations. Because of this characteristic, this software is often referred to as “black box” software.[16]

All medical products, including AI-enabled software, can fail in unusual, unpredictable ways when the mechanism of action is not understood. In software that incorporates machine learning, failures may be partly due to unrecognized site-specific patterns or “clues” present in the training data, which can result in suboptimal performance when the system is deployed in new and different settings. For example, when researchers trained algorithms on pooled x-ray image data from sites with varying pneumonia prevalence, they found that the algorithms most likely used site-specific features in the images to significantly influence the resulting prediction, rather than simply relying on the underlying pathology. Because of these site-specific influences, the algorithmic models were not consistently generalizable to new health systems.[17]

When software is not explainable, rigorous performance testing can be performed to better understand the risks of the software. Prospective testing within the planned workflow is necessary to understand real-world product performance and whether the system may fail in unexpected ways. In addition, information provided at point-of-use, such as the certainty of a particular result, or what factors were weighed most heavily, may help users understand when to trust a particular result in the absence of a true explanation. The level of explanation or performance data necessary also can be calibrated as a function of risk posed by the software’s intended use.

Categories of Information Surrounding AI-Enabled Clinical Decision Software

Categories of information exist that various stakeholders might want for AI-enabled clinical decision software products: how a software system fits into clinical workflow; what type of AI it is; how it was developed; how it works; and other information that may be useful to know about individual results (see **Figure 3**).

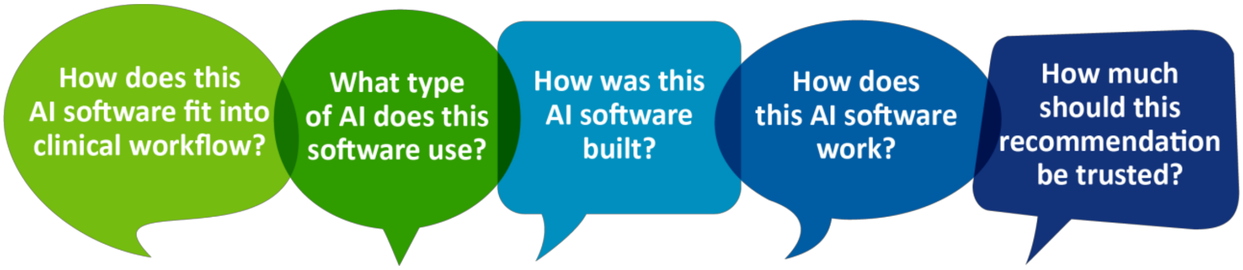

How does this AI software fit into clinical workflow?
What type of AI does this software use?
How was this AI software built?
How does this AI software work?
How much should this recommendation be trusted?

Figure 3. Categories of information for AI-Enabled Clinical Decision Software. *Various stakeholders throughout the total product lifecycle of a software product will want specific information of what the software does and how it fits into the workflow, what type of AI is used and how it was built, as well as information about how it works and when to trust the results.*

Information about the intended user of the software and how it relates to clinical decision-making should always be disclosed to all stakeholders. This baseline understanding should include the intended purpose and user of the device, and the significance of the result or recommendation to the user's clinical decision-making.

Relatedly, all stakeholders will need to understand whether an AI-enabled software product is designed to assist or automate a clinician's decision-making. If the software notifies a doctor of a possible medication interaction, or highlights certain areas of an x-ray for further review, the software is assistive and the final decision rests with the provider.

In contrast, autonomous AI-enabled software products diagnose or treat patients directly. This automatic action may occur through hardware that is part of the system, such as an implantable cardiac defibrillator that analyzes heart rhythm and sends an electrical shock to the heart. Alternatively, software may convey results to other users, who may not be trained to make the decision themselves, but who are still capable of taking next steps based on the results. It should be noted that the distinction between these two categories may not be clear cut, as there are multiple gradations in between.

To evaluate AI-enabled software, stakeholders also need to know what type of AI it uses. Is the software rules-based or data-based? If it is data-based, what learning algorithms were used to develop the software? Different types of algorithms are more suitable for different types of problems and data, similar to how certain statistical methods are more appropriate for certain types of analyses.[18]

Additionally, stakeholders need to know if AI-enabled software developed with machine learning is locked or continuously updating. Locked AI-enabled software means data-based techniques are used during development, but the software does not continuously learn and change over time. We are not aware of any continuously learning standalone software products that have been cleared or approved by FDA. However, continuously learning software products might be in use for administrative or population health purposes that are not under FDA authority.

How was this AI software built?

Certain stakeholders might want more detailed information about the software development process as well. Full transparency for data-based AI could mean algorithmic transparency, which would include the code for the learning algorithm, as well as hyperparameters, training data, and other information needed to reproduce the algorithm(s) used in the software. For locked algorithms, transparency could also include model transparency—disclosure of the exact function or functions that are used to compute how all inputs are weighted and combined to produce the outputted recommendation. Stakeholders may also ask for detailed information about the training data, including how it was labeled.

As discussed further below, patents can, at least in theory, provide intellectual property protection even in the case of such full transparency.[**] However, difficulties in enforcing patents, and a desire on the part of some patent applicants to attempt to maintain both patent and trade secrecy protection over the same information, may make applicants reluctant to provide full transparency. Recent U.S. Supreme Court patent eligibility cases have made patenting of both medical diagnostics and software more difficult. When companies do not have secure patent protection, they may rely even more heavily on trade secrecy to protect their investment in innovation.

One context in which trade secrecy may be particularly important is training data. Patents and copyright do not extend to raw data. The restrictions on information flow required by trade secrecy law may also align with privacy-related legal prohibitions against disclosing training data that contains personal health information (PHI).

However, even if manufacturers are reluctant to disclose training datasets, summary information on patient populations represented, including demographics, social determinants of health, geographical region, comorbidities, and genetic markers, will still be useful. Any data curation, inclusion/exclusion criteria for adding patient data to the training dataset, and clear methodologies for how the data was labeled should also be part of this summary, and be incorporated into device labelling. Summary information on patient populations used for training should shed at least some light on potential biases and on whether the training population resembles the patient population of interest to the stakeholder.

How does this AI software work?

A common question that stakeholders have regarding novel medical products is: how does the product work? For traditional medical devices, information regarding how to reproduce the device (of the sort that should be disclosed in patents) should also provide insight into how the device works. Unfortunately, in the case of data-based software, information required to reproduce the algorithm driving a software product may not be helpful for human understanding of what that software is doing.

A true explanation delineates exactly how the software product will process input data to produce a result. Software that utilizes rules-based AI can always give “true” explanations, and certain types of machine learning or product designs also can provide some explainability. For black box algorithms,

[**] Patent doctrine requires that the information disclosed in the patent provide the basis for reproduction—specifically, that it shows “one skilled in the art” how to make and use the claimed invention.

statistical techniques that can produce a “likely” explanation are also being explored.[19]

Because of this limited explainability, detailed performance data should become more important to stakeholders. Indeed, rigorous evidence around performance should be required by all stakeholders, regardless of the type of AI used (although requirements on rigor may differ based on the risk posed by the AI). It is therefore critical for stakeholders to clearly communicate what type of performance data is being asked for and given. For example, studies involving data-based AI should include information regarding whether performance results are coming only from a validation dataset that was separated from the original training data before training began, or from a completely independent dataset collected from a different source and/or at a different time.[20] Testing on a completely independent dataset will shed light on whether software performance depends on data features or patterns specific to the sites from which the training data was collected.

Stakeholders also should understand whether testing was retrospective or prospective, and whether the product was tested in the environment and within the workflow in which it is intended to be used.[21] A 2017 JASON report on AI for Health and Health Care recommends that rigorous procedures be developed for approving and accepting AI-enabled software into clinical practice, including testing and validation approaches for AI algorithms to evaluate performance under different conditions.[22]

Furthermore, adopters need information on how software inputs should be structured and defined. For example, does the software only work with images from particular manufacturers or models of imaging equipment? Having this information will enable stakeholders to understand if their own data can be used effectively by the software. Prior to adoption, potential adopters may also want to consider testing the software on their own data to evaluate local performance.

How much should this recommendation be trusted?

Finally, clinicians need appropriate information at the point-of-use about software system results to determine how heavily to weigh them in their decision-making. This information can include the certainty of the software for a specific result or the key input features that led to a specific recommendation. Users also may find it useful to have information about whether their patient significantly differs demographically or medically from the training and testing population. It is important that software systems be designed to communicate such information quickly, and in readily understandable ways to accommodate clinicians’ busy schedules. However, FDA has cautioned against using labeling beyond what is typical in clinical settings. Information provided should be in line with the labeled use of the product and, for automated systems, information that users are not trained to interpret should be avoided as is may be counter-productive.

Governance Structures for Information Flow Across the Total Product Lifecycle

Once we understand the categories of information surrounding AI-enabled software, it is important to understand the regulatory and institutional frameworks that govern how this information might be requested or supplied by stakeholders at each point of the total product lifecycle (development, regulation, adoption, monitoring, and use). The following sections address governance issues surrounding information flow. The discussion is based on literature review, database searches,

Attachment #9

perspectives provided during meetings hosted by the Center of Innovation Policy at Duke Law and the Duke-Margolis Center for Health Policy, and individual stakeholder interviews.

Development

Patent Law

Patent law requires applicants to provide a disclosure that enables scientists of “ordinary skill” to “make and use” the invention. Relatedly, applicants must provide a “written description” about the structure of the invention they are claiming. Under the patent system, this disclosure, which mirrors the scientific research and publication norm of reproducibility, is the *quid pro quo* that inventors provide to society in exchange for a time-limited right to control both direct competition and cumulative innovation in their area of invention.

While disclosure through patents can occur, the U.S. Patent and Trademark Office does not always enforce disclosure requirements. Moreover, applicants often file for patents early in the R&D process, before a full understanding of the invention has been achieved.[23]

Legal and ethical challenges unique to AI-enabled health software may impede disclosure by developers. First, software patent law is highly unsettled (as mentioned earlier), so companies might not feel confident in the protections that patents otherwise confer. Second, training data might contain personally identifiable information or information that could be combined with other data to re-identify the individuals who were the source of that data. The potential for identification (or re-identification) raises privacy concerns, including potential violations of the Health Insurance Portability and Accountability Act (HIPAA) depending on the type of data used. Finally, in the case of AI-enabled software, although reproducibility allows some scientists to have confidence in the veracity of their results, this does not mean that the model is comprehensible to all scientists, let alone to other stakeholders.

To investigate patent disclosure further, we examined the patents associated with several prominent data-based AI software products recently cleared by the FDA.[24] These included the QuantX software for reading MRIs to detect abnormalities suspicious for breast cancer; the Viz.AI ContaCT device for detecting, and triaging, suspected large vessel occlusions in an emergency room context; and the IDx-DR software for analyzing retinal images to provide a primary care physician with a recommendation regarding whether diabetic retinopathy had been detected. We found that the patent disclosures associated with these products contained at most only a brief, highly general, discussion of training data, the training process, or criteria used for validation.

Funding

We also examined the issue of venture capital (VC) funding, particularly in light of Supreme Court decisions that make patenting of AI-enabled clinical decision software more challenging. Our data indicate that the Court decisions have not deterred VC investment. To the contrary, as with AI-enabled health generally,[25] VC investment in AI-enabled clinical decision software has risen in recent years.[26] That said, one of the venture capitalists we interviewed did indicate that greater ability to patent would further increase investment in small machine learning firms. Each of the venture capitalists we interviewed viewed developer secrecy over training data and model details as key mechanisms for protecting investment in innovation.[27]

Attachment #9

FDA Regulation

FDA defines medical devices as instruments used in the diagnosis, cure, mitigation, treatment, or prevention of disease, that can affect the structure or function of the body through non-chemical means. This definition includes certain types of software, termed “Software as a Medical Device (SaMD)” that are “intended to be used for one or more medical purposes and to perform these purposes without being part of the hardware of the medical device.”[28] Thus far, AI-enabled SaMD have been cleared under either the 510(k) pathway for devices substantially similar to other devices on the market or through a de novo classification for novel low-to-moderate risk devices. FDA has published multiple documents on SaMD. These papers include discussion of both CDS and AI-enabled SaMD, and have not suggested that there will be systematic differences in how AI-enabled software will be evaluated relative to other software. Below, we review these documents to understand the types of information that that FDA may request from manufacturers as part of regulatory review.

As an initial matter, it is important to note that not all clinical decision software is SaMD. Under the 21st Century Cures Act (Cures Act) of 2016, software that is not SaMD includes software that presents institution-specific best practices, facilitates access to treatment guidelines, or software that acts in an administrative or quality improvement capacity. The Cures Act also establishes a somewhat complex scheme for determining what types of clinical decision support (CDS) software are, and are not, subject to FDA authority.[††]

Since 2016, FDA has worked to interpret the CDS software provisions of the Cures Act. In September 2019, FDA released an updated draft of its CDS Software guidance, which removes certain types of CDS software from FDA authority (FDA calls these “non-device CDS software”).

The Cures Act specifies several criteria that determine whether a CDS software product is a medical device and therefore under FDA authority. The first criterion relates to the required input data. Any product that uses a “medical image or signal from an in vitro diagnostic device, or pattern or signal from a signal acquisition system” as an input remains under FDA authority (“device CDS software”).

Even if the CDS software does not use imaging or signal data, it must pass additional tests in order to fall outside of FDA authority. The software should be intended for the purpose of “displaying, analyzing, or printing medical information about a patient” in order to support or provide recommendations “to a health care professional about the prevention, diagnosis or treatment of a disease or condition”. Further, it must allow the “health care professional to independently review the basis for recommendations that software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.”

The “independent review” criterion has proved especially challenging to interpret. In an example from the appendix to its 2019 guidance, FDA states that software developed with machine learning could meet this criterion if “the logic and data inputs for the algorithm and the criteria for [the

[††] In its 2019 draft CDS guidance, FDA limits the term clinical decision support (CDS) to software “supporting or providing recommendations to an [healthcare professional], patient, or caregiver.” Software that drives or automates diagnosis or treatment decisions would be considered a medical device, but not CDS software. The term “clinical decision software” used in this paper is intentionally broad, to encompass both device and non-device CDS, as well as software that drives or automates diagnosis or treatment.

recommendations] were explained and available to the [health care professional].” The FDA’s statement suggests that AI-based software that is not able to provide a human-comprehensible explanation for how the software works or details about specific recommendations will remain under FDA authority. As for FDA’s reference to data inputs being available to the user, it is unclear if machine-learning software that uses large numbers of input elements will be able to comply with that requirement in a way that reasonably allows independent review.

For CDS software products under FDA authority, FDA will use a risk-based approach and take into consideration four factors (see **Table 1**):

1. The significance of the software result in clinical decision-making;
2. The clinical context of the health care situation;
3. The type of user (health care professional versus patient or caregiver); and
4. The ability of that user to independently review the basis for the recommendation.

The guidance states that the International Medical Device Regulators Forum (IMDRF) framework will be used to assess the first two factors.

Table 1. Summary of regulatory policy for CDS software functions. Modified from FDA’s 2019 CDS draft guidance document.[‡‡]

CDS software that “informs” clinical decision-making	User: Healthcare Providers		User: Patient/Caregiver	
	Can Independently Review	Can Not Independently Review	Can Independently Review	Can Not Independently Review
Non-Serious	Not a medical device	Enforcement discretion	Enforcement discretion	Oversight focus
Serious	Not a medical device	Oversight focus	Oversight focus	Oversight focus
Critical	Not a medical device	Oversight focus	Oversight focus	Oversight focus

Because FDA will incorporate these four factors (the IMDRF categories regarding clinical context and the significance of the information, the ability to independent review recommendations, and the intended user) into their risk assessment, clear labels would be extremely useful. The intended user is already a prominent part of the label, but the specific clinical context and the significance of the information as defined in the guidance are often less clear.

Beyond interpreting the Cures Act, FDA is also examining the possibility of a new regulatory model for software. Announced in July 2017,[29] the Software Pre-Certification (“Pre-Cert”) Pilot Program is meant to help inform “the development of a future regulatory model that will provide more streamlined and efficient regulatory oversight of software-based medical device.”[30] The program is being developed in response to FDA’s recognition that its traditional approach to regulating medical devices “is not well

[‡‡] According to a November 2019 FDA webinar, “enforcement discretion” indicates that, at this time and based on FDA’s current understanding of the risks of these devices, FDA does not intend to enforce compliance with applicable device requirements.

suited to the faster iterative design, development, and type of validation" used for many SaMD products.[31]

The latest working model, updated in January 2019, explains that companies that have met the pre-certification qualifications will still go through a review pathway determination for individual software products, based on the risk of the software. The working model lists product-level elements that may contribute to the review pathway determination, which include "an explanation of how the software works" as well as "instructions and limitations on use" and the "critical features/functions of the SaMD that are essential to the intended significance of the information" to decision-making.[32] FDA lists the clinical algorithm as one of the product-specific elements in the streamlined review process description, including mechanism of action (although the term is not defined). As such, it is currently unclear whether a lack of explainability will affect the risk assessment of a software product under Pre-Cert or how the review pathway selected might change if some of those product-level elements are absent. As the pilot continues, more details might be shared to clarify these questions.

The Pre-Cert model states that "validation of the clinical algorithm is of primary importance and would be fully described and would include both protocols for testing and results demonstrating performance." In the April 2019 discussion paper on AI/ML and continuous learning, FDA emphasizes the need to have "large, high-quality, and well-labeled data sets" to have a robust algorithm.

Stakeholder interviews suggest that FDA is not asking companies for full training data or detailed information about the algorithms for AI-enabled software products developed with machine learning. Instead, companies have shared summary information on training data and have provided more detailed information on clinical study data, methodology, and results for FDA assessment. Our interviews indicate that although companies are not averse to disclosing details regarding the underlying model to regulatory agencies, they are hesitant to hand over detailed training data that they view as a trade secret.

Manufacturers also report that FDA is interested in understanding the user experience. Relevant information includes the amount or type of information the end user receives as well as the significance of the software recommendation and fit for the end user.

Manufacturers in our stakeholder interviews report their experiences with FDA as positive. Stakeholders view FDA's proposed Pre-cert Program as a positive sign that FDA is thinking deeply about how regulatory policy should change to foster new innovations while maintaining patient safety. To keep up with device review, manufacturers also acknowledge the need to increase FDA's ability to recruit and retain relevant talent or expertise. FDA has already released statements about its efforts to increase the "number and expertise of digital health staff at FDA"[33] and to create partnerships with medical product centers, academic stakeholders, and other partners in order to "improve the ability of FDA reviewers and managers to evaluate products that incorporate advanced algorithms and facilitate the FDA's capacity to develop novel regulatory science tools."[34]

Stakeholders also agreed that adopters view FDA clearance/approval as a positive indicator of efficacy. We will discuss adoption more in the next section.

Adoption and Use

The next step in the product lifecycle is two-fold: the adoption and implementation of a software product into a provider system, and the decision by a health care provider and patient at point of use to incorporate the software recommendation into their decision-making. Convincing healthcare systems to adopt and use AI-enabled software will depend on the software's perceived or demonstrated ability to improve health outcomes, the costs and financial benefits seen by adopters of the technology, how well it can be integrated into clinical workflows, alignment to the standard of care, and the relevant law and regulations on tort liability.

Depending on where the product is deployed, different types of information may be required for health systems, providers, and patients to trust these technologies enough to adopt and use them. [35] For initial adoption decisions, data showing the software can improve the system's overall patient population health may be an important factor. At point of use, however, the certainty of the output or the logic and key inputs leading to the recommendation may be more important to clinicians, as well as what medical or other patient factors may affect the accuracy of the recommendation. Such information can help them discern when specific recommendations may be more or less relevant for the particular patient in front of them.

Adoption

Multiple stakeholders mentioned that FDA approval or clearance was a helpful mark of quality and effectiveness. However, stakeholders also used other information when making a decision to adopt a software product. Our interviews suggest that decision-makers are most interested in information pertaining to performance, including sensitivity and specificity analyses.[§§] Health systems may also ask for explanations on how the software works and will improve day-to-day clinical processes.

Provider system stakeholders also spoke about the need for guidelines and systems to properly assess new AI-enabled products. A user guide released in November 2019 delineates how provider systems should evaluate diagnostic products developed with machine learning.[36] The authors recommend starting the assessment with a determination that the machine learning method is appropriate giving the function of the resulting software and the type and amount of data used to train the algorithm. The number and regularization of parameters should also be assessed to determine if overfitting[***] may be a concern.

Next, the algorithm should be validated and the validation methods should be examined. Was the validation dataset completely separate from the datasets used to train and tune the algorithm? Is the reference standard high quality? This latter question can be a challenge when there is no gold standard for comparison.[37] With results that seem "too good to be true" or if unexpected associations or correlations are found, the performance can be validated in additional patient cohorts to "ensure that the results are not due to artifacts in the machine learning systems, confounding factors, or flaws in the study design."[38] Repeatability and reproducibility of the software recommendations should also be

[§§] Sensitivity and specificity analysis are generally used in medical diagnosis to determine the ability of a test to correctly identify the true positive rate or those with a disease (also known as sensitivity) in addition to the true negative rate, or the ability of the test to correctly identify those without the disease (also known as specificity).

[***] Overfitting occurs when an algorithm is built to match the training data too closely. Because the algorithm creates rules for "noise" that is only present in that specific dataset, the software is not generalizable to other data sets.[39]

Attachment #9

assessed, by examining how small changes in input data affects the outcomes, as well as how input data from different hardware, operators, and protocols may affect real-world performance.

One of the concerns frequently discussed in academic circles is whether health care should demand "explainable" software from developers or if "black box" software is acceptable. AI enthusiasts commonly say many clinicians (including themselves) use medical devices daily that they don't understand. However, such use generally occurs with the knowledge that many experts (such as the manufacturers, FDA, and possibly even a technical assessment committee within the provider system) do understand how the device works and can test for potential complications based on that understanding. This is different from black box algorithms, where there is no explanation that even experts can understand about how the software is analyzing the input data to come to outputs.

It should be acknowledged that it is not unusual for the mechanism of action of a medical product to not be fully understood, and this is generally addressed with rigorous testing to alleviate concerns with safety and efficacy. In an editorial published in January 2020, researchers argue that a practical solution could be to demand different levels of explainability based on use case and the balance of benefit and risk.[40] The authors also recommend rigorous performance studies and local pilot testing before and after implementation if adopting "black box" software.[41]

Almost all the stakeholders interviewed stressed that AI-enabled clinical decision software can enhance workflows, positively influence care decisions, and improve outcomes.[†††] In order to achieve these goals, information must flow in both directions. Provider systems can help developers by being more open about their processes and needs, while developers can bring in people who are well-versed in these systems to help consult during the development process. In addition, best practices are needed on how developers can efficiently provide evidence of improved workflow and outcomes, or take on risk in value-based outcome arrangements with provider systems when there are questions regarding how much realized value will be gained by the patients or system.

Even with evidence of clinical utility, stakeholders recognized, as previously discussed, multiple factors that might affect whether a specific software will work effectively with a particular health system's patient population, data systems, and workflow. Therefore, some of the interviewed provider systems test all algorithms with data from provider system patient populations before making a final decision to adopt a system. However, even those who did testing noted that not all health care systems have adequate resources for testing.

Stakeholders repeatedly mentioned algorithmic performance may degrade over time due to the ever-changing nature of input data. This makes the ability to continually monitor the performance of the algorithm critical. Despite concerns, none mentioned systematic processes outfitted to do this type of monitoring. Additionally, despite increasing interest in AI-enabled software, machine-learning systems have not yet achieved widespread use in health care systems. A January 2020 Technology Review Insight survey found only 10 percent of health care institutions have deployed one or more AI applications, with another 17 percent having deployed one or more AI pilot projects.[42] However, another 45 percent of the institutions surveyed are in the process or are planning to deploy AI in the next 2 years. Notably, of the institutions that use or plan to use AI, 74 percent plan to develop their own customized AI algorithms.

[††††††] In fact, the standard of care could evolve to require that the performance of the provider by augmented by software.

While ensuring that algorithms are trained on appropriate patient population and workflows is key, customization leaves the institution with the sole responsibility of monitoring performance over time and updating the software as needed. For healthcare systems that are very large, there may need to be customization within the system itself based on the location in which the product is deployed.

Minimizing security and privacy risks through proper controls or data governance also will be key to dynamic health system operationalization. Interviewees stressed implementing processes in a way that seamlessly integrates with the user experience and fosters patient trust by safeguarding vital information.

Clinician Acceptance and Use

More than one stakeholder interview transitioned into a conversation about workforce training and the user experience. As hospitals strive to cultivate AI systems and continue to evolve, algorithms should relay critical information about individual recommendations to clinicians in a user-friendly manner. However, clinicians also need to be provided ample opportunity to understand basic foundational concepts. The April 2019 European Commission Ethics Guidelines for Trustworthy AI speak to this need for human agency and oversight stating that users should be "given the knowledge and tools to comprehend and interact with AI systems to a satisfactory degree and, where possible, be enabled to reasonably self-assess or challenge the system."[43] The June 2018 American Medical Association (AMA) policy on the use of augmented intelligence (also known as AI) in health care underscores the need for thoughtfully designed, high-quality, and clinically validated AI-enabled software, and the ability for the provider to "understand AI methods and systems sufficiently to be able to trust an algorithm's predictions."[44] However, without a proper knowledge base, clinicians might not be able to effectively work with, or manage, the AI system, or know which specific questions they can ask to gain appropriate insight.

As a first step, clear and accessible product labeling for clinicians to refer to during use can be crucial to allowing the user to fully assess risks and biases that might arise from the algorithmic training process.[45] Medical device labels include information on the benefit-risk profile as well as indications for proper use. Stakeholders familiar with the FDA approval process proposed that key elements might include aggregated stats about the patient population used to train the model (demographics of training and validation) in addition to information about accuracy of the algorithm tested on completely independent validation sets.

While label information is important, stakeholder discussions also revealed that information about specific recommendations might be more valuable to busy clinicians at the point of care. Suggestions included incorporating information about how a software's key input factors influencing the recommendation and information to help clinicians understand how many "patients like theirs" are included in the training data. Stakeholders agreed that default information should be limited and quick to digest visually rather than requiring users to scroll through dense text, however some suggested that users should be able to "click" to get more detail.

The type, level of software autonomy, and degree of information provided to clinicians will affect the amount of liability they might be willing to accept (especially when the results given by the AI system differ from their own clinical judgement). Some stakeholders indicated that users (and health systems) are hesitant to take on undue risk and invest in AI-enabled systems without fully understanding how liability will play out in the long term and with whom the responsibility lies.

The authors of an October 2019 study examine possible scenarios in which the recommendation from the software does or does not differ from standard of care, the clinician follows or rejects the recommendation, whether the patient outcome is good or bad, and what the potential liability may be in each case. Their work suggests that, at least until the use of medical AI itself becomes part of the standard of care, "the 'safest' way to use medical AI from a liability perspective is as a confirmatory tool to support existing decision-making processes, rather than as a source of ways to improve care."[46] The authors recommend that clinicians protect themselves by gathering information and asking clinical societies to develop best practices in how to evaluate both a new AI product overall and individual recommendations from that product, as well as ensuring that products have been thoroughly vetted before procurement. Furthermore, the authors suggest that physicians should ask questions from their malpractice insurers about use of AI-enabled clinical decision software. Changes might be required to both coverage contracts and liability laws as AI-enabled software becomes more widespread.

Patient Acceptance

The data on patient acceptance are mixed. A September 2019 survey revealed that about 45 percent of respondents said they were interested in their physician using AI to help with a diagnosis, due to the potential for a more accurate diagnosis, a reduction in human error, and/or faster treatment decisions.[47] However, a May 2019 paper found that patients were less likely to use or pay for a service if the health care was provided by an AI system instead of a human provider.[48] Although these patients did not believe the AI provided inferior care, the patients were skeptical that the AI was able to provide care that was tailored to their circumstances and unique patient profile.[49]

The amount or level of information patients want can differ based on whether the software is assistive or automated, and might affect how willing they are to embrace certain technologies. Typically, patients want AI that assists clinicians as opposed to automating them—acting as a complement instead of a replacement, especially with sensitive treatments or lasting interventions.[50] A January 2019 study conducted by Deep Mind and RSA revealed that increased ease of understanding with respect to information conveyed to the patient does not necessarily translate into increased levels of trust. Of those respondents surveyed, 36 percent were likely to support automated AI systems if they were able to request an explanation of the steps or processes it took to come to the decision, with only 20 percent indicating increased support of the technology if it were explainable to an individual with no technical expertise.[51]

Conclusion

Stakeholders require substantial information about AI-enabled software to effectively harness its benefits and mitigate risk. Some information regarding AI-enabled software is comparable to information stakeholders need to know about traditional medical products. However, AI-enabled software can present additional informational demands. Moreover, unique business concerns and technical challenges may at times create mismatches between information regulators and adoptersdesire and information developers are willing or able to provide. Our work examined where these mismatches may exist and what information regulators and adopters of AI-enabled software may accept in lieu of traditional information.

Our research suggests that, as an empirical matter, conflicts over trade secrecy have not been a significant issue so far. We found that regulators and adopters' informational needs vary based on how recommendations produced by AI-enabled software are used in clinical decision-making, as well as the clinical context. Furthermore, for the moment, regulators and adopters' expectations align with the amount of information currently disclosed by manufacturers. Manufacturers are reluctant to share training data or disclose details of trained models, but they are generally willing to share summary information on both. Thus far, stakeholders have not been pushing for more detailed information.

In part, the current congruence of stakeholder expectations may arise because most products used today are low- to medium-risk. As more autonomous and higher risk products that may require more trust emerge, expectations could diverge and tensions arise. For example, given developers' reluctance to share training data and full model details with third parties, including the FDA, high-risk scenarios where access to such information was important may create tensions. More troubling is the possibility that disputes have not yet arisen because, even now, adopters are asking for insufficient information. For example, in contravention of emerging best practices, some adopters do not appear to be asking for performance data gleaned from a dataset collected completely independently from the initial training dataset.

Our research also shows that basic education about AI-enabled products is necessary for stakeholders, particularly end users, to understand the type of information they need to safely use AI-enabled clinical decision products. Policy makers, hospital systems, and researchers will need to work together to provide end users with educational resources that promote understanding the information needed during their decision-making process. Currently, FDA is working on expanding and fortifying its workforce through active recruitment efforts. Hospital systems need to consult with clinicians and internal technological assessment committees to create systematic plans for evaluating products and educating their workforce. And though there has been an increase in literature on how to effectively evaluate AI-enable products in health care, it might be useful for a centralized third-party to act as a repository for these evaluations—although this will not account for challenges around site-specific data and workflow issues.

Below are initial recommendations on information that should be shared as stakeholders explore, evaluate, adopt, use, and monitor emerging AI-enabled products:

- Provider systems should be open about their internal process challenges and informational needs so manufacturers are better able to develop products that solve real problems and fit into the health system work flow. In parallel, manufacturers need to bring in experts who are well-versed in health system workflows and curating products for the user experience. Manufacturers also need to show evidence of the clinical utility of their product, not just the accuracy of the results.
- As products emerge that have a higher risk profile, procedures should be developed by which information considered by developers to be a trade secret (e.g. training data and model details) may need to be shared with trusted third parties (e.g., the FDA) that can evaluate the information.
- Conveying performance data on an independent test set, information regarding the certainty of the recommendations, and, if technically possible, key weighted factors in the algorithm's

decision-making process can increase stakeholder trust as they evaluate the product and determine whether to adopt or use it.

- Information about the intended use (such as the purpose, user, significance of decision, level of autonomy given, patient population) should always be disclosed publicly, in addition to summary information about the training data, labeling methodology, and testing or validation process.
- Manufacturers need to clearly define data input requirements, including the structure and definition of each data element, so adopters can understand if the algorithm can be used effectively with their patient population and workflows. Defining the expected clinical context of the data collection may also be important.
- Stakeholders should develop a set of best practices and recommendations on how to best evaluate a new AI-enabled software product, including guidelines for how to thoroughly vet products before procurement.

Finally, because AI-enabled software can fail or break in unexpected ways, manufacturers and health systems should work together to monitor system performance after implementation, including updating as needed, and share information about product limitations and adverse or near-miss events.

AI has the potential to streamline workflows, increase job satisfaction, reduce spending, and improve health outcomes. A 2020 survey demonstrates that 89 percent of healthcare executives believe that AI is already creating efficiencies in health systems, and 91 percent believe it has the potential to increase patient access to care.[52] Estimates also show that AI can help address about 20 percent of unmet clinical demand.[53,54] However, to achieve these goals responsibly and cultivate long term success, ensuring that the right information is shared with the right stakeholder at the right time will be essential.

References

[1] Bresnick, J. (2018). “Top 12 Ways Artificial Intelligence Will Impact Healthcare.” *Health IT Analytics.* Retrieved from https://healthitanalytics.com/news/top-12-ways-artificial-intelligence-will-impact-healthcare

[2] Accenture. (2017). “Artificial intelligence: healthcare’s new nervous system.” Retrieved from https://www.accenture.com/t20171215T032059Z__w__/us-en/_acnmedia/PDF-49/Accenture-Health-Artificial-Intelligence.pdf

[3] Duke-Margolis Center for Health Policy. (2019). “Current State and Near-Term Priorities for AI-Enabled Diagnostic Support Software in Health Care.” Retrieved from https://healthpolicy.duke.edu/sites/default/files/atoms/files/dukemargolisaienableddxss.pdf

[4] Sullivan, H.R., & Schweikard, S.J. (2019). “Are current tort liability doctrines adequate for addressing injury caused by AI?” *AMA J Ethics.* Retrieved from https://journalofethics.ama-assn.org/article/are-current-tort-liability-doctrines-adequate-addressing-injury-caused-ai/2019-02

[5] Duke-Margolis Center for Health Policy. (2018). “Characterizing RWD Quality and Relevancy for Regulatory Purposes.” Retrieved from https://healthpolicy.duke.edu/sites/default/files/atoms/files/characterizing_rwd.pdf

[6] Gianfrancesco, M.A., et al. (2018). “Potential biases in machine learning algorithms using electronic health record data.” *JAMA Intern Med. Retrieved from* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6347576/

[7] Obermeyer, Z., et al. (2019). “Dissecting racial bias in an algorithm used to manage the health of populations.” *Science.* Retrieved from https://science.sciencemag.org/content/366/6464/447

[8] Ibid.

[9] FDA. (2019). “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD).” *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/122535/download

[10] FDA. (2017). “Digital Health Innovation Action Plan.” *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/106331/download

[11] FDA. (2018). “Developing Software Precertification Program: A Working Model.” *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/113802/download

[12] FDA. (2019). “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD).” *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/122535/download

[13] Jilani, T.N., & Sharma, S. (2019). “Trihexyphenidyl.” *StatPearls.* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK519488/

[14] Rosenbaum, S.B., & Palacios, J.L. (2019). “Ketamine.” *StatPearls.* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK470357/

[15] Conway, C.R., & Xiong, W. (2018). “The Mechanism of Action of Vagus Nerve Stimulation in Treatment-Resistant Depression: Current Conceptualizations.” *The Psychiatric Clinics of North America.* Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/30098653

[16] Duke-Margolis Center for Health Policy. (2019). “Current State and Near-Term Priorities for AI-Enabled Diagnostic Support Software in Health Care.” Retrieved from https://healthpolicy.duke.edu/sites/default/files/atoms/files/dukemargolisaienableddxss.pdf

[17] Zech, J.R., et al. (2018). “Variable generalization performance of a deep learning model to detect pneumonia in chest radiographs: A cross-sectional study.” *PLOS Medicine.* Retrieved from https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1002683

[18] Crown, W.H. (2015). “Potential Application of Machine Learning in Health Outcomes Research and Some Statistical Cautions.” *Value in Health*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1098301514047913

[19] Turek, M. (2018). “Explainable Artificial Intelligence (XAI).” *Defense Advanced Research Projects Agency.* Retrieved from https://www.darpa.mil/program/explainable-artificial-intelligence

[20] Liu, Y., et al. (2019). “How to Read Articles that use Machine Learning User’s Guide to the Medical Literature.” *JAMA.* Retrieved from https://jamanetwork.com/journals/jama/fullarticle/2754798

[21] Topol, E. (2019). “High-performance medicine: the convergence of human and artificial intelligence.” *Nature Medicine.* Retrieved from https://www.nature.com/articles/s41591-018-0300-7

[22] JASON. (2017). “Artificial Intelligence for Health and Health Care.” *The MITRE Corporation.* Retrieved from https://www.healthit.gov/sites/default/files/jsr-17-task-002_aiforhealthandhealthcare12122017.pdf

[23] Cotropia, C.A. (2009). “The Folly of Early Filing in Patent Law.” 61 Hastings L.J. 65.

[24] Rai, A.K., et al. (2020). “Accountability, Secrecy, and Innovation in AI-Enabled Clinical Decision Software.” *Journal of Law and the Biosciences.* In press.

[25] Ibid.

Attachment #9

[26] Ibid.

[27] Ibid.

[28] IMDRF SaMD Working Group. (2013). "Software as a Medical Device (SaMD): Key Definitions." *IMDRF.* Retrieved from http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

[29] FDA. (2017). "Digital Health Innovation Health Plan." *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/106331/download

[30] FDA. (2019). "Developing Software Precertification Program: A Working Model (v1.0)." *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/119722/download

[31] FDA. (2017). "Digital Health Innovation Health Plan." *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/106331/download

[32] FDA. (2019). "Developing Software Precertification Program: A Working Model (v1.0)." *U.S. Department of Health and Human Services.* Retrieved from https://www.fda.gov/media/119722/download

[33] Gottlieb, S. (2018). "Transforming FDA's approach to digital health." Retrieved from https://www.fda.gov/news-events/speeches-fda-officials/transforming-fdas-approach-digital-health-04262018

[34] Gottlieb, S. (2019). "The Role of Real-World Evidence in Regulatory and Value-Based Payment Decision-Making." *Remarks made at Bipartisan Policy Center.* Retrieved from https://bipartisanpolicy.org/events/the-role-of-real-world-evidence-in-regulatory-and-value-based-payment-decision-making/

[35] Duke-Margolis Center for Health Policy. (2019). "Current State and Near-Term Priorities for AI-Enabled Diagnostic Support Software in Health Care." Retrieved from https://healthpolicy.duke.edu/news/white-paper-release-current-state-and-near-term-priorities-ai-enabled-diagnostic-support

[36] Liu, Y., et al. (2019). "How to read articles that use machine learning." *JAMA*. Retrieved from https://jamanetwork.com/journals/jama/article-abstract/2754798

[37] Adamson, A.S., & Gilbert Welch, H. (2019). "Machine learning and the cancer-diagnosis problem—no gold standard." *NEJM*. Retrieved from https://www.nejm.org/doi/full/10.1056/NEJMp1907407

[38] Liu, Y., et al. (2019). "How to read articles that use machine learning." *JAMA*. Retrieved from https://jamanetwork.com/journals/jama/article-abstract/2754798

[39] Hanelman, G.S., et al. (2029). "Peering into the black box of artificial intelligence: evaluation metrics of machine learning methods." *AJR*. Retrieved from https://www.ajronline.org/doi/full/10.2214/AJR.18.20224

[40] Wang, F., et al. (2020). "Should health care demand interpretable artificial intelligence or accept "black box" medicine?" *Annals of Internal Medicine.* Retrieved from https://www.acpjournals.org/doi/10.7326/M19-2548?searchresult=1

[41] Ibid.

[42] MIT Technology Review Insights. (2019). "The AI effect: how artificial intelligence is making health care more human." Retrieved from https://mittrinsights.s3.amazonaws.com/ai-effect.pdf

[43] High-Level Expert Group on Artificial Intelligence. (2019). "Ethics guidelines for trustworthy AI." Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1#Human%20agency

[44] American Medical Association. (2018). "Augmented intelligence in health care: report 41 of the AMA Board of Trustees." Retrieved from https://static1.squarespace.com/static/58d0113a3e00bef537b02b70/t/5b6aed0a758d4610026a719c/1533734156501/AI_2018_Report_AMA.pdf.

[45] Geis, J.R., et al. (2019). "Ethics of artificial intelligence in radiology: summary of the joint European and North American multisociety statement." Retrieved from https://www.jacr.org/article/S1546-1440(19)30944-5/pdf

[46] Ibid.

[47] UnitedHealth Group. (2019). Retrieved from https://www.unitedhealthgroup.com/newsroom/2019/2019-09-26-consumer-sentiment-survey-tech.html

[48] Longoni, C., et al. (2019). "Resistance to medical artificial intelligence." *JCR*. Retrieved from https://academic.oup.com/jcr/article-abstract/46/4/629/5485292?redirectedFrom=fulltext

[49] Longoni, C., & Morewedge, C.K. (2019). "AI can outperform doctors, so why don't patients trust it?" *HBR*. Retrieved from https://hbr.org/2019/10/ai-can-outperform-doctors-so-why-dont-patients-trust-it

[50] Tran, V., et al. (2019). "Patients' views of wearable devices and AI in healthcare: findings from ComPaRe e-hort." *Npj Digital Medicine.* Retrieved from https://www.nature.com/articles/s41746-019-0132-y?utm_source=STAT+Newsletters&utm_campaign=f5d8c45344-health_tech_COPY_01&utm_medium=email&utm_term=0_8cab1d7961-f5d8c45344-149547853

[51] Balaram, B., et al. (2019). "Artificial intelligence: real public engagement." *RSA.* Retrieved from https://www.thersa.org/globalassets/pdfs/reports/rsa_artificial-intelligence---real-public-engagement.pdf

[52] KPMG. (2020). "Living in an AI world." Retrieved from https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/living-in-ai-world.pdf

Attachment #9

[53] Insights Team. (2019). “AI and healthcare: a giant opportunity.” *Forbes.* Retrieved from https://www.forbes.com/sites/insights-intelai/2019/02/11/ai-and-healthcare-a-giant-opportunity/#2ea1e3be4c68

[54] Accenture. (2017). “Artificial intelligence: healthcare’s new nervous system.” Retrieved from https://www.accenture.com/t20171215T032059Z__w__/us-en/_acnmedia/PDF-49/Accenture-Health-Artificial-Intelligence.pdf

Attachment #10

McKinsey & Company

Healthcare Systems and Services Practice

The era of exponential improvement in healthcare?

Technology-driven innovation holds the potential to improve our understanding of patients, enable the delivery of more convenient, individualized care—and create $350 billion–$410 billion in annual value by 2025.

By Shubham Singhal and Stephanie Carlton

May 2019

Attachment #10

Executive summary

Healthcare advances have delivered great benefits to society, bringing material improvements in average life spans and quality of life.[1] Yet these improvements have come at a cost—an ever-expanding portion of the US GDP is being consumed by healthcare expenses.[2] Could technology, enabling delivery of healthcare advances while improving affordability, be part of the solution? We have reviewed the evidence, done the math, and identified technology-enabled use cases that could create between $350 billion and $410 billion in annual value by 2025 (out of the $5.34 trillion in healthcare spending projected for that year[3]).

Technology-driven progress can be quite expensive in the early days as initial R&D costs are amortized. The next five to seven years are likely to require a sustained upshift in investment to unlock the potential of these assets, and the strategies used to pursue this potential could have significant effects on both their effectiveness and rate of adoption. Once progress gets underway and the exponential improvements seen typically with information and communication technologies take root, at-scale costs could drop rapidly. For instance, the cost of genome sequencing has dropped significantly over the past decade and a half.

Emerging technologies are reshaping healthcare in multiple ways—how consumers access it, how and which providers deliver it, and what health outcomes it achieves. We identify nine emerging technologies: connected and cognitive devices, electroceuticals, targeted and personalized medicine, robotics, 3D printing, big data and analytics, artificial intelligence, blockchain, and robotic process automation. Some of these innovations are specific to healthcare; others are more advanced in nonhealthcare sectors but hold tremendous potential in healthcare. Use cases and sources of value from these emerging technologies do not exist in isolation. Innovators are considering how to integrate them and deliver transformative change.

As we look toward the future of healthcare, there are four industry-level changes that could disrupt healthcare value pools as they exist today: modernized transaction and data infrastructure; radically more efficient medical supply chain; faster, more effective therapy development; and new, personalized, and intuitive healthcare ecosystems.

Perhaps the most significant change could be the creation of intuitive and personalized ecosystems of care centered around patients and their families, into which their community of medical and social caregivers would be integrated. Such ecosystems would make possible the delivery of the right type and amount of care, in the right setting, at the right time. The ecosystems could be enabled by a combination of:

— *holistic and longitudinal patient data sets* to integrate today's fragmented information from social systems, financial resources and systems, home-care and self-care monitoring, activities of daily life, and traditional modalities of care,

[1] For the past three years, life expectancy has declined, largely because of a broader set of behavioral health issues. (See Murphy SL et al. Mortality in the United States, 2017. National Center for Health Statistics Data Brief, no. 328. November 2018. cdc.gov.)
[2] See Exhibit 1 in Singhal S, Coe E. The next imperatives for US healthcare. McKinsey white paper. November 2016.
[3] Office of the Actuaries in the Centers for Medicare & Medicaid Services. National health expenditure projections, 2018–2027. cms.gov.

Attachment #10

- *advanced analytics and AI personalization engines* to generate insights for patients and their community of caregivers,
- *continuum of care interaction models*, ranging from digital solutions to close-to-home services to traditional facilities, based on individual needs,
- *device-enabled, autonomous care* and cognitive engagement,
- *real-time refinement of individualized care solutions* and cognitive engagement through an AI-enabled interaction medium, and
- *seamless integration of monitoring and care* from clinical caregivers, social and community structures, and family members.

We are aware that predictions of healthcare disruption have been made for decades. And that traditional healthcare dynamics—resulting from ingrained consumer mindsets, highly-trained clinician behaviors, entrenched stakeholder interests, a complex regulatory framework, and the fragmented nature of the market—have affected and may continue to affect adoption of progress.

Realizing this value will require disruptors—incumbents and attackers alike—to understand the technologies available today, develop clear ways to use the technologies with evidence for how they will create value, implement effective human change management strategies, and execute disciplined implementation plans. Whether they do so will answer the question of whether we are entering an era of technology-enabled disruption in healthcare.

Attachment #10

The era of exponential improvement in healthcare?

Table of Contents

Healthcare advances have delivered great benefits to society, bringing material improvements in average life spans and quality of life.[1] Yet these improvements have come at a cost—an ever-expanding portion of the US GDP is being consumed by healthcare expenses, as medical inflation continues to outstrip GDP growth and inflation in the rest of the economy.[2] Going forward, might we be able to deliver healthcare advances while improving affordability? Exponential progress through technology-driven innovation could have deflationary impact on the cost of healthcare while delivering new medical advances. Our analysis shows that there are practical use cases that together have the potential to deliver between $350 billion and $410 billion in annual value by 2025 (out of the $5.34 trillion in healthcare spending projected for that year[3]).

Many information and communication technologies have followed predictably exponential improvement and growth trajectories.[4] Moore's law is a well-recognized example.[5] Technology-based home- and ride-sharing services have grown exponentially to disrupt established businesses by delivering more affordable access to lodging and transportation and greater utilization of capital assets. With the mapping of the human genome and digitization of medical data, healthcare could now be subject to the same type of exponential progress. For instance, the cost of genome sequencing has dropped significantly over the past decade and a half. Adoption of both DNA testing and telehealth, while still small, is growing swiftly (Exhibit 1). Such exponential progress can seem benign at first, with seemingly minimal change to the status quo, but an explosion of progress then follows. To illustrate, if the rate of improvement doubles every year, it would take seven years to get from 0.01 to 1 percent—but only another seven years to get to 100 percent.

Exponential progress, however, is not preordained. Technology-driven progress can be quite expensive in the early days as initial R&D costs are amortized. We see this today in the cost of emerging genomics-based treatments. Additional investments are necessary to underwrite a longitudinal, fully integrated patient data infrastructure,[6] as well as the development of advanced analytics and machine learning capabilities. How will these investments be funded and early high costs absorbed? Over the past decade, the amount of private equity and venture capital deployed in pharmaceutical, biopharma, health technology, and digital health assets has grown (Exhibit 2). The next five to seven years are likely to require a sustained upshift in investment to unlock the potential of these assets, and the strategies used to pursue this potential could have significant effects on both their effectiveness and rate of adoption. Once progress gets underway and the exponential improvements seen typically with information and communication technologies take root, at-scale costs could drop rapidly.

Within healthcare, however, traditional dynamics—resulting from ingrained consumer and clinician behaviors, entrenched stakeholder interests, a complex regulatory framework, and the fragmented nature of the market—have affected, and may continue to affect, the adoption of new technology-enabled approaches and innovation. Indeed, it is possible that if these traditional dynamics predominate, exponential progress may not come to pass in the foreseeable future.[7] These forces certainly make it difficult to predict the pace of change. Nonetheless, the ascent of technology-driven disruption in other industries (consider online retail platforms, home- and ride-sharing services, and personalized, on-demand media)

[1] For the past three years, life expectancy has declined, largely because of a broader set of behavioral health issues. (See Murphy SL et al. Mortality in the United States, 2017. National Center for Health Statistics Data Brief, no. 328. November 2018. cdc.gov.)

[2] See Exhibit 1 in Singhal S, Coe E. The next imperatives for US healthcare. McKinsey white paper. November 2016.

[3] Office of the Actuaries in the Centers for Medicare & Medicaid Services. National health expenditure projections, 2018–2027. cms.gov.

[4] Kurzweil R. *The Singularity is Near: When Humans Transcend Biology.* 2005.

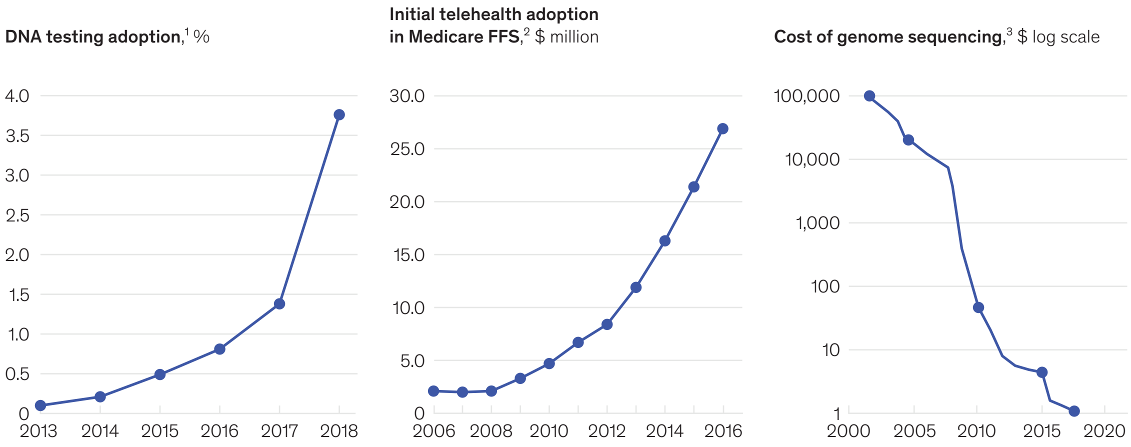
[5] Moore's law is an observation made by Intel's founder Gordon Moore that the number of transistors on a chip doubles each year, whereas the costs are halved.

[6] For example, additional investments are needed to establish common data standards across providers and to ensure good data hygiene following the adoption of electronic health records.

[7] We acknowledge that, in general, portfolio momentum from a zealous focus on growth out-competes the market, but it is possible for incumbents to invest in the wrong place at the wrong time during periods of industry disruption. Atsom Y. How growth champions thrive even in stagnating markets. McKinsey white paper. August 2017.

Exhibit 1

Progress in healthcare can be exponential



FFS, fee-for-service.

[1] Consumer adoption of major testing companies (Ancestry.com and 23andme) within the US, assuming one test per person.

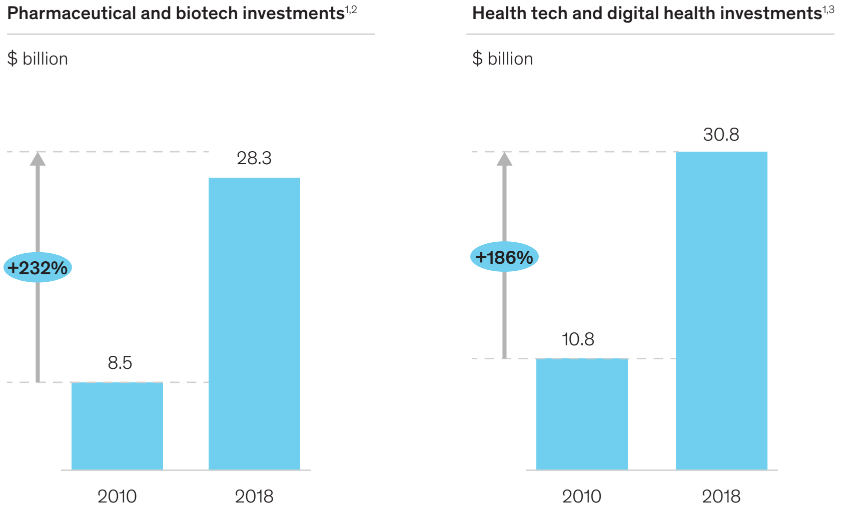
[2] Based on Medicare physician fee schedule claims for distant site telehealth visits per 1,000 FFS Part B beneficiaries. Although the data shown here is only a small fraction of Medicare's budget (approximately $770 billion for 2019), it illustrates the increased utilization of telehealth services.

[3] Based on National Human Genome Research Institute data.

Source: Medicare Payment Advisory Committee, *Report to the Congress: Medicare Payment Policy*, March 2018; National Human Genome Research Institute, DNA sequencing costs: Data, April 25, 2018; Regaldo A, "2017 was the year consumer DNA testing blew up," *MIT Technology Review*, February 12, 2018

Exhibit 2

Sizeable investments are being made to fuel healthcare innovation



[1] Includes venture capital and private equity funding sources only and excludes all PIPE (private investment into public entity) investments.

[2] Sum of investments in biotechnology, healthcare discovery tools, drug delivery, drug discovery, and pharmaceutical categories.

[3] Health tech is defined as mobility and information technology companies that aid care delivery while decreasing costs; digital health is defined as hardware and software solutions to track health and enable patient-physician communications.

Source: PitchBook data (2010–2018); McKinsey analysis demonstrates that underestimating the pace and extent of change can be more problematic for incumbents than overestimating it. At a minimum, technology innovators are reshaping consumer expectations for healthcare: today's consumers expect personalized, device-enabled, intuitive 24/7 service that revolves around convenience and empowerment in all areas of their lives.[8,9]

To understand the potential for industry disruption, consider: clinical care, an important and primary focus for the healthcare industry to date, explains about 15 percent of overall health outcomes; social determinants, health behaviors, and genetics account for the rest.[10] Consider further that the average patient will, in his or her lifetime, generate about 2,750 times more data related to social and environmental influences than to clinical factors (Exhibit 3). In a data- and technology-enabled world, it is not a stretch to imagine that whole new business models could be created by nonhealthcare players to deliver superior health outcomes.

In the remainder of this article, we address three topics: What emerging technologies have the potential to reshape healthcare? What is the potential value at stake? What disruptive changes might happen?

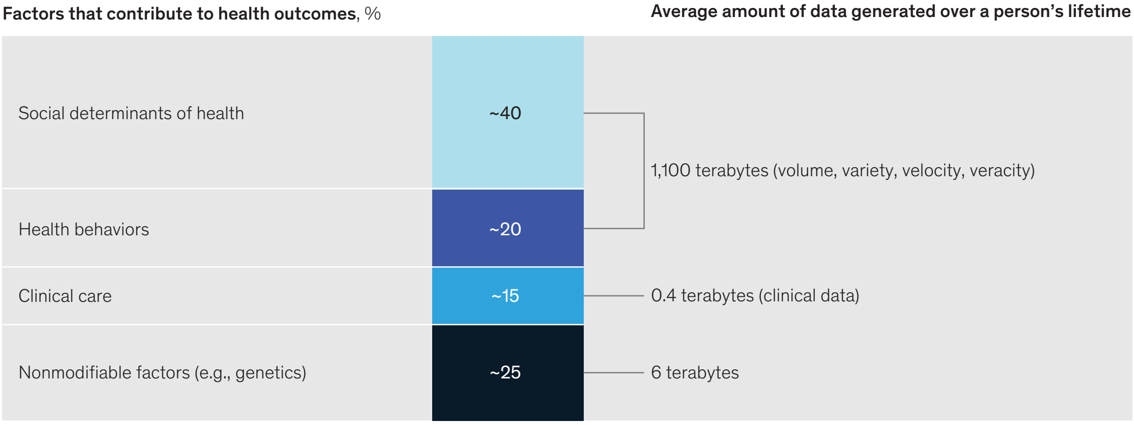
What emerging technologies could reshape healthcare?

Healthcare innovation is occurring at an unprecedented pace. The Center for Drug Evaluation and Research in the Food and Drug Administration (FDA) approves double the average annual number of novel drugs as it did a decade ago.[11] Among the therapies approved in 2017, 15 were first-in-class, indicating that they had a unique mechanism of action; another 18 address rare or orphan diseases. Some could dramatically improve the precision of diagnostics and the

[8] Cordina J et al. Healthcare consumerism 2018: An update on the journey. McKinsey white paper. July 2018.
[9] Cordina J et al. Debunking common myths about healthcare consumerism. McKinsey white paper. December 2015.
[10] This estimate is based on a McKinsey analysis of data from a range of organizations (for example, Centers for Disease Control and Prevention, Association of State and Territorial Health Officers), academic studies (for example, Hood CM et al. County health rankings: Relationships between determinant factors and health outcomes. *American Journal of Preventive Medicine*. 2016;50(2):129–35), and other groups, including the Robert Wood Johnson Foundation (see Medicaid's role in addressing social determinants of health. Robert Wood Johnson Briefing Series. Issue 5. February 2019).
[11] Center for Drug Evaluation and Research. Advancing health through innovation: 2017 new drug therapy approvals. US Food and Drug Administration. 2018. fda.gov.

Exhibit 3

Societal issues have a major impact on consumer health



Source: Bureau of Labor Statistics; Robert Wood Johnson Foundation; IBM Watson (Latts L. *The age of big data and the power of Watson.* European Medicines Agency presentation. Updated April 1, 2017); McKinsey analysis

Attachment #10

Novel drugs are just one of nine emerging technologies that are reshaping healthcare in multiple ways.

ability to personalize treatments (for example, through biomarkers), which could help reduce the significant variability in outcomes achieved by standard therapies. In the past two years, truly individualized treatments have been approved, ones that genetically modify patients' immune cells to battle leukemia and lymphoma.[12] Curative therapies could substantially alter the nature and length of delivery system demands from patients with chronic illnesses, potentially creating downstream savings. Furthermore, the care delivery requirements of some novel treatments could make possible more convenient and affordable care in or closer to patients' homes.

Novel drugs are just one of nine emerging technologies that are reshaping healthcare in multiple ways—how consumers access it, how and which providers deliver it, and what health outcomes are achieved. Some of these innovations are specific to healthcare; others are more advanced in nonhealthcare sectors but hold tremendous potential in healthcare.

Connected and cognitive devices. Portable, wearable, ingestible, and/or implantable devices can monitor health information, engage patients and their community of caregivers, and deliver therapies autonomously.

Electroceuticals. Small implantable devices can alter the nervous system's electrical impulses to treat a variety of diseases.

Targeted and personalized medicine. Novel drug therapies that use a patient's own cells or deliver targeted genetic material can often treat disease more successfully than small-molecule or protein-effector drugs can.

Robotics. Next-generation robots could enable minimally invasive approaches and ease the physical burden of surgeries. Advanced robotics could also expand automation beyond specimen and material transport within the hospital to facilitate instrument handling and other tasks within the operating room.

3D printing. This technology can produce customized, 3-dimensional structures composed of biological and industrial materials, in the process creating organ replacements, personalized prosthetics, and precision medication dosages.

Big data and analytics. Platforms and applications that store, transmit, and analyze continuously expanding medical data sets can be used to identify patients who are candidates for highly targeted therapies. In the future, physiological data recorded by robots during procedures could be leveraged to improve both medical education and surgical planning. As more data becomes readily available—some sources suggest an annual growth rate in available data of 48 percent[13]—the opportunity to better collect data and translate it into actionable insights is increasing.[14]

Artificial intelligence (AI). Technologies that convert analytical insights into cognitive engagement solutions can enhance diagnosis, improve predictive interventions, and optimize clinical productivity.

Blockchain. This decentralized digital ledger technology holds the potential (with clear and simple use cases[15]) to enable more secure transactions, more confidential patient data sharing, and more democratized data access,

[12] Aptekar J et al. Precision medicine: Opening the aperture. McKinsey white paper. February 2019.
[13] Stanford medicine 2017 health trends report. Harnessing the power of data in health. June 2017. med.stanford.edu.
[14] Admittedly, data privacy and patient privacy regulations will influence the extent to which this can be done.
[15] Higginson M et al. Blockchain's Occam problem. McKinsey white paper. January 2019.

which could allow other technologies to better leverage data (for example, provider directories that can be rapidly updated with new network structures).

Robotic process automation (RPA). The automation of repetitive tasks (including the majority of claims processing) via simple rules or heuristics has the potential to rapidly enhance productivity.

While we cannot predict precisely how quickly each technology will emerge and scale in healthcare, each has the potential to have significant impact over the next five to seven years. Among the factors that will influence the speed of change are the pace of innovators, the appetite of incumbents for change, and the rate at which regulations adapt to technology.

What is the potential value at stake?

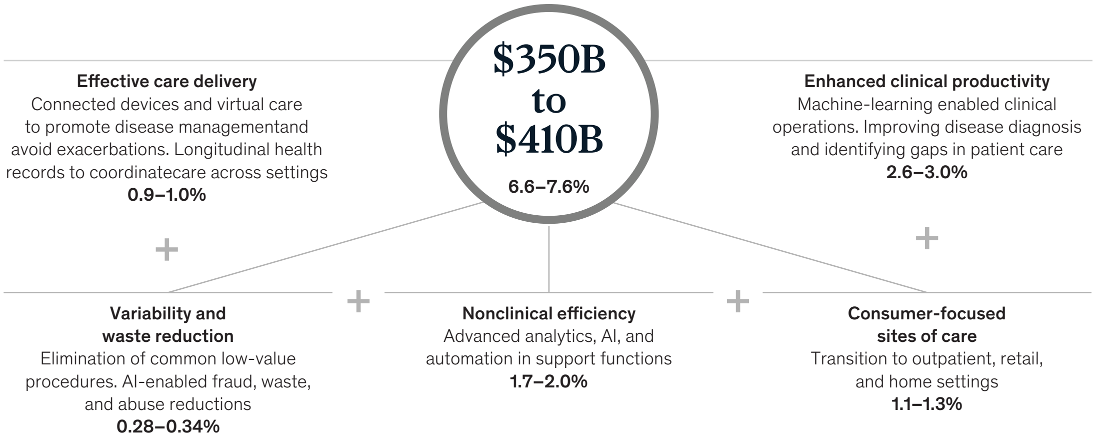
By 2025, US healthcare spending is expected to top $5.34 trillion.[16] Recently, we identified a $284-billion to $550-billion opportunity for value creation from the application of best practices to improve healthcare productivity and market function.[17] Integration of the nine emerging technologies in healthcare could create an additional $350 billion to $410 billion in value annually by 2025 (Exhibit 4). This value creation could be offset, in part, by increased demand due to improved affordability (that is, if individual healthcare services are more affordable, utilization could rise, which could reduce gross savings to the system). Nevertheless, these value creation levers may have the potential to contain the growth in health expenditures to be in line with broader economic growth.

This estimate of value creation reflects a net effect and the beginning of paradigm shifts in how healthcare is delivered. New curative therapies, for example, might be more expensive than current drugs but hold the potential to improve outcomes for patients with previously unaddressable conditions and lower the costs

[16] Office of the Actuaries in the Centers for Medicare & Medicaid Services. National health expenditure projections, 2018–2027. cms.gov.
[17] Singhal S, Coe E. The next imperatives for US healthcare. McKinsey white paper. November 2016.

Exhibit 4

Technology-driven value estimates are based upon potential use cases



$350B to $410B

6.6–7.6%

Effective care delivery
Connected devices and virtual care to promote disease managementand avoid exacerbations. Longitudinal health records to coordinatecare across settings
0.9–1.0%

Enhanced clinical productivity
Machine-learning enabled clinical operations. Improving disease diagnosis and identifying gaps in patient care
2.6–3.0%

Variability and waste reduction
Elimination of common low-value procedures. AI-enabled fraud, waste, and abuse reductions
0.28–0.34%

Nonclinical efficiency
Advanced analytics, AI, and automation in support functions
1.7–2.0%

Consumer-focused sites of care
Transition to outpatient, retail, and home settings
1.1–1.3%

AI, artificial intelligence.
Source: McKinsey analysis

Attachment #10

Technology could accelerate the shift... to consumer-focused sites of care.

associated with current care delivery approaches.[18] We have estimated the shifts in costs[19] and incorporated them into our net impact estimate of technology-driven healthcare disruption. However, it is also possible that new curative therapies could deliver or make possible other economic benefits that might eventually affect the shifts in spending. For instance, our estimate did not assess the potential impact to economic productivity and lifetime healthcare costs that could be realized through better health or increased longevity.

We outline below why we believe this value creation is possible in several categories, based on our review of the evidence, identification of use cases, and quantitative analysis. The estimates of value creation are discrete and do not overlap across categories; in each category, they are shown as percentages to better inform the strategic planning efforts of incumbents and innovators alike. The question to be considered in realizing this value is: Will healthcare incumbents and attackers advance the business strategies to capture the potential value? Put another way, will the technology overcome the inertia of the healthcare industry and consumers of care under the status quo?

Consumer-focused sites of care optimization

We believe the combination of the nine emerging technologies discussed above can enable greater innovation in moving care into or close to patients' homes. Consumers increasingly expect this for healthcare services[20] now that they can shop, connect with friends, bank, and access personalized, on-demand media content this way. Care delivered in or close to a patient's home—geographically or in lower-acuity settings that feel like home—is usually less expensive and reduces the risk of nosocomial infections (which provides an additional opportunity for care delivery savings). As regulatory and market pressures evolve, technology could accelerate the shift from traditional hospital settings to consumer-focused sites of care, such as ambulatory surgery centers, retail clinics, and homes.[21,22] For some conditions, at-home management may lower costs by 19 to 32 percent.[23] Home infusion and observation care models are expected to grow by more than 10 percent over the next five years, as predictive analytics improves its ability to identify patients most likely to benefit from home-based care and connected devices allow clinicians to remotely monitor

[18] Over the long term, the combination of these technologies could also affect life expectancy, but the costs and savings associated with longer life expectancy were not analyzed as part of this report.

[19] To estimate the potential impact of these advances, we identified the therapeutic areas and conditions with both high medical spending and unmet need: leukemia, hemophilia, macular degeneration, sickle-cell disease, some breast cancers, some lung cancers, hypercholesterolemia, and depression. We then identified potential therapies in the FDA pipeline and sized the value that could be realized through approval and launch of innovative therapies that could meet these needs by 2025. Using commercial claims data and adjusting for overall population characteristics, we determined the impact of these therapies on spending across all major categories of care (for example, hospital, post-acute, pharmaceutical).

[20] Cordina J et al. Healthcare consumerism 2018: An update on the journey. McKinsey white paper. July 2018.

[21] Note: The scope of procedures appropriate in ambulatory surgery centers (ASCs) supports a potential shift away from traditional hospital care: for 2019, CMS recommended 172 additional procedures to join 3,910 existing procedures eligible for reimbursement through ASCs. (See Centers for Medicare & Medicaid Services. Medicare program: Proposed changes to hospital outpatient prospective payment and ambulatory payment systems and quality reporting programs. CMS-1695-P. 2019. Also see Addendum AA from Centers for Medicare & Medicaid Services. Medicare program: Hospital outpatient prospective payment and ambulatory surgical center payment systems and quality reporting programs. CMS-1678-FC. 2018.)

[22] Merchant Medicine. Reports, data licensing and research. merchantmedicine.com.

[23] Klein S et al. The hospital at home model: Bringing hospital-level care to the patient. The Commonwealth Fund. August 2016; Cryer L et al. Costs for 'hospital at home' patients were 19 percent lower, with equal or better outcomes compared to similar inpatients. *Health Affairs*. 2012;31(6):1237–43.

patients.[24] Increasingly sophisticated data and analytics could, over time, accelerate this transition in care delivery by giving patients clearer information in advance to guide choices related to their site of care.

Many novel treatments could also enable more efficient care delivery. For instance, once protocols are well established for genomics-based treatments, the delivery requirements (which primarily involve infusion and observation) could move into or close to home. While this has not happened rapidly for every new therapy—as slow adoption of home hemodialysis has shown—we describe below some of the achievable savings where we see strong evidence of potential delivery structure and economic impact.

For our economic estimate, we sized the potential value from shifting sites of care for three major care transition areas with broad potential for impact: transferring avoidable emergency department care to urgent care centers or retail clinics, increasing the volume of procedures performed outside the traditional hospital setting (for example, in ambulatory surgery centers), and moving some facility-based care to the home. Based on recent academic and industry literature on the opportunity at stake in each of these three care transition areas, we applied comparable technology adoption rates and assumed that approximately half of the possible value could shift to consumer-focused sites of care by 2025. Several other related shifts in care—for instance, the movement of infusion therapy from the clinic to the home or in-home post-acute care recovery—were not included in our estimate but have the potential to augment this value. In each case, we estimated value using commercial claims data, adjustments for overall population characteristics, and evidence-based assumptions on savings; we then aggregated the projected value across the three areas to determine the total opportunity. Taken together, shifting care to lower-acuity sites could generate annual value equivalent to between 1.1 and 1.3 percent of national health expenditures by 2025.[25,26]

Enhanced clinical productivity

The healthcare industry lags behind other industries in its ability to “do more for less.”[27] Yet, the introduction of technology-enabled interventions could dramatically improve productivity in clinical settings (as well as patient outcomes) and eventually lead to the automation of activities related to care delivery. Critical to improving productivity—rather than simply spending more money on technology—is identifying a clear set of use cases and evaluating their potential return on investment (ROI). Examples of such use cases already exist. Robotic technology, for instance, is being used to increase the precision of percutaneous coronary interventions that improve circulation to the heart, which reduces demands on the clinical staff, lowers stent usage in patients, and decreases radiation exposure during the procedure for both groups. Miniature electroceutical devices that can stimulate nerves in the human body are being developed to treat diabetes, arthritis, and asthma. Other tools that could enhance clinical productivity include:

— cognitive engagement platforms designed to improve wellness among all patient segments and, specifically, increase adherence among patients with chronic or high-acuity conditions

— automated analytics tools that enhance diagnosis by utilizing data aggregated across the population

[24] Home infusion therapy market expected to be worth US $25 billion by 2024. MarketWatch. August 31, 2018. marketwatch.com.
[25] This estimate does not account for the potential additional savings that could be achieved by lowering in-hospital disease transmission.
[26] This analysis used simplifying assumptions: that the shift to lower-acuity sites would not lead to overutilization of services; that this shift could lead to a reduction in hospital emergency department usage, which could prompt some hospitals to reevaluate their cost distribution structures; and that technology will improve consumer incentives to select lower-cost, lower-acuity settings for care.
[27] Singhal S, Coe E. The next imperatives for US healthcare. McKinsey white paper. November 2016.

— AI-based assistance in patient diagnosis and routine administrative duties to enhance physician productivity

These three examples are just a subset of the opportunities to enhance clinical productivity. We completed a more holistic sizing of these opportunities, building on research from the McKinsey Global Institute (MGI).[28] An evaluation of technology-enabled potential suggests a subset of 25 healthcare-specific use cases that would improve clinical productivity, consumer satisfaction, and health outcomes. Using MGI's proprietary estimates of the impact of the various analytics tools in different categories of spending, we sized these use cases across the US healthcare industry and applied adoption rates similar to historical adoption rates for healthcare technologies, such as electronic health records. We estimate that technology-driven improvements in clinical productivity, consumer satisfaction, and health outcomes could deliver net savings equal to 2.6 to 3.0 percent of national health expenditures by 2025.

Variability and waste reduction

Uneven adherence to evidence-based medicine is common in US healthcare. Nearly three-quarters of today's physicians identify the ordering of unnecessary tests as a serious problem.[29] Technologies available today can be used to unlock the potential of improving clinician and patient awareness of rapidly evolving medical evidence, enabling more precise and efficient diagnostics, and ensuring tighter adherence to established and personalized treatment protocols (with an associated reduction in activities that add little value in improving health outcomes). For instance, low-value procedures (such as unnecessary or duplicative imaging) could be eliminated from standard practice using longitudinal patient records and at-home monitoring.[30,31] The integration of AI and new record-keeping technologies such as blockchain into billing and claims processes could reduce the incidence of fraud, waste, and abuse, yielding additional value.

For our economic assessment, we began with MGI's proprietary estimates of proven ways to use analytic tools to reduce fraud, waste, and abuse, and then applied these use cases to US healthcare spending (again, assuming adoption rates would be similar to historical healthcare technology adoption rates). We also used professional medical association standards to identify low-value services (tests, treatments, or procedures), as well as state-level data on the prevalence of unnecessary tests and procedures, to size the potential impact of reducing variability and waste by minimizing the use of ten of those services. Using this evidence base, we estimated the potential value at stake and then refined our estimate based on the potential for technology to enable clinician behavior change. Technological advances, for instance, could dramatically reduce the frequency of unnecessary screening by giving clinicians access to longitudinal patient records. In addition, we built on the MGI research to analyze the potential impact of decreasing fraud, waste, and abuse through the use of improved algorithms. We estimate that the total annual value delivered by technology in these two areas is likely to be about 0.28 to 0.34 percent of national health expenditures by 2025.

Nonclinical efficiency

The introduction of AI and other analytics tools could enhance nonclinical efficiency as well as clinical efficiency, largely through automation of routine administrative tasks. For instance, payers that have applied RPA in areas like claims adjudication and provider network life-cycle management have achieved significant improvements in productivity through a reduction in manual activities. One healthcare-focused technology company recently introduced an enterprise-scale blockchain solution that can process up to

[28] Bughin J et al. Notes from the AI frontier: Modeling the impact of AI on the world economy. McKinsey Global Institute. September 2018.
[29] ABIM Foundation. Research Report. Choosing Wisely. 2017. choosingwisely.org.
[30] Truven Commercial claims database.
[31] ABIM Foundation. Choosing Wisely. abimfoundation.org.

Attachment #10

The introduction of AI…could enhance non-clinical [and] clinical efficiency, largely through automation of routine administrative tasks.

about 50 million events daily and allows hospitals and physician practices to track the real-time status of claims from submission to remittance.[32]

Building on the MGI research, we sized a set of use cases in which automation could be used to improve nonclinical efficiency in areas such as hiring and retention, marketing, pricing, and procurement. Each use case was evaluated for its readiness for application in healthcare settings (for example, how automation of broader core business functions or procurement could be relevant for providers) and then scaled across the US healthcare industry, adjusted for source of coverage, and adjusted again to account for historical healthcare technology adoption rates. We estimate that these and other use cases could deliver annual value equal to approximately 1.7 to 2.0 percent of national health expenditures by 2025.

Effective care delivery

We see the potential for technology to alter current care pathways via longitudinal patient-centric records, real-time patient monitoring, and remote and autonomous patient engagement. Apple's well-known partnership with a growing number of health systems, including Stanford Medicine, Partners HealthCare, and Johns Hopkins, is beginning to integrate longitudinal health records and supplemental data sources into a patient-controlled smart phone ecosystem, which could lead to a paradigm shift from "provider-centric" to "patient-centric" data structures.[33] The FDA has cleared two mobile medical Apple Watch "apps" that can take electrocardiograms and monitor pulses for irregular heart rhythms.[34] One start-up is using an AI-enabled diagnostic system to detect diabetic retinopathy based on images of patients' eyes and pooled data; the goal is to help primary care providers more rapidly diagnose the condition without extensive testing. These new technologies are making possible both better integration of care between patients and caregivers and fully autonomous care (similar to the technology available for an artificial pancreas that monitors glucose and then provides appropriate insulin dosing). In addition, a number of AI-enabled chatbot technologies, designed to help young adults deal with anxiety and depression through intelligent conversational engagement, are starting a paradigm shift—AI cognitive engagement replacing a role played by licensed clinicians.

We believe the highest ROI will stem from tying these technologies to the care pathways for chronic conditions, given that spending on chronic conditions continues to increase. For instance, heart disease, diabetes, and hypertension together account for about $575 billion annually in national health expenditures.[35]

To estimate potential savings, we prioritized seven high-spend pathways that might benefit significantly from technology: heart disease, diabetes, hypertension, chronic obstructive pulmonary disease, cancer,

[32] Miliard M. Change Healthcare's enterprise blockchain tech now available for hospitals, practices, payers. Healthcare IT News. January 8, 2018. healthcareitnews.com.

[33] Apple. Empower your patients with Health Records on iPhone. apple.com.

[34] U.S. Food and Drug Administration. Statement from FDA Commissioner Scott Gottlieb, MD, and Center for Devices and Radiological Health Director Jeff Shuren, MD, JD, on agency efforts to work with tech industry to spur innovation in digital health. FDA. September 12, 2018. fda.gov.

[35] Centers for Disease Control and Prevention. Diabetes at work: Calculate what diabetes costs your business, high blood pressure fact sheet, and heart disease fact sheet. cdc.gov.

Attachment #10

depression, and general primary care. These pathways were selected from an evidence-based review of over 300 studies and academic physician interviews.[36] For each pathway, we determined average episode spending based on a proprietary algorithm applied to commercial claims data (adjusted for overall US population size, sources of coverage, and other characteristics), as well as historical healthcare industry technology adoption rates. This approach allowed us to identify the current extent of care variations in the pathways, as well as the potential reduction in variation that might be achieved by particular levers associated with these technologies. (For example, the availability of devices that enable clinician connectivity could reduce episode spending variations, particularly on outpatient or home care services.) This estimate of value assumes that technology could equip physicians with better awareness of the latest medical evidence and improve access to better data about current and historical patient conditions. We calculate that by rethinking how technology can improve care for these and other high-spend pathways, annual value of 0.9 to 1.0 percent of national health expenditures could be realized by 2025.

What disruptive changes might happen?

Each of these use cases and sources of value does not exist in isolation. Innovators are considering how to integrate them and deliver transformative change. As we journey toward the future of healthcare, we see four potential industry-level changes that could disrupt healthcare value pools as they exist today:

Modernized transaction and data infrastructure. The integration of technologies such as blockchain digital ledgers, RPA, cloud computing, and AI could automate risk prediction and utilization management (capabilities currently delivered by payers). It could also result in a patient-centric data infrastructure (for example, longitudinal patient data could be integrated with nonclinical sources of patient data and then parsed by machine learning). In addition, the entire billing and insurance transaction infrastructure could be standardized, automated, and streamlined. Such a transaction infrastructure could be operated by a few large-scale entities, become a broad industry utility—or both.

Radically more efficient medical supply chain. Technologies such as real-time patient monitoring, RPA, AI, and drone deliveries could anticipate patients' diagnostic and treatment needs, then deliver supplies to patient homes or targeted clinical settings precisely when needed. The result could be stronger supply chain management, fewer user errors, better patient adherence, and improved health outcomes. This reorganization of the supply chain, however, could be disruptive to the established business models of wholesale and retail distributors across the pharmaceutical and medical products industries.

Faster, more effective therapy development. The time needed to demonstrate the safety and efficacy of innovative therapies could potentially be reduced by the combination of two things: the ability to analyze longitudinal patient records (which will become even more powerful once the records can be integrated with genomic data and data on social and environmental factors) and the ability to test new therapies on 3D-printed tissue. Historical data (and eventually historical and contemporaneous data) could be used to predict the likelihood of outcomes, and new therapies could be tested on 3D-printed tissue in real time. This type of simulation of traditional clinical trials could significantly reduce the extent and duration of those traditional trials. As an aside, traditional clinical trials themselves could be made more effective and efficient by leveraging advanced analytics and AI. The resulting reduction in both the cost and timeline of therapy development could enhance competition, thereby increasing the affordability of the therapies.

[36] Interviews with clinicians at Harvard and Johns Hopkins medical schools.

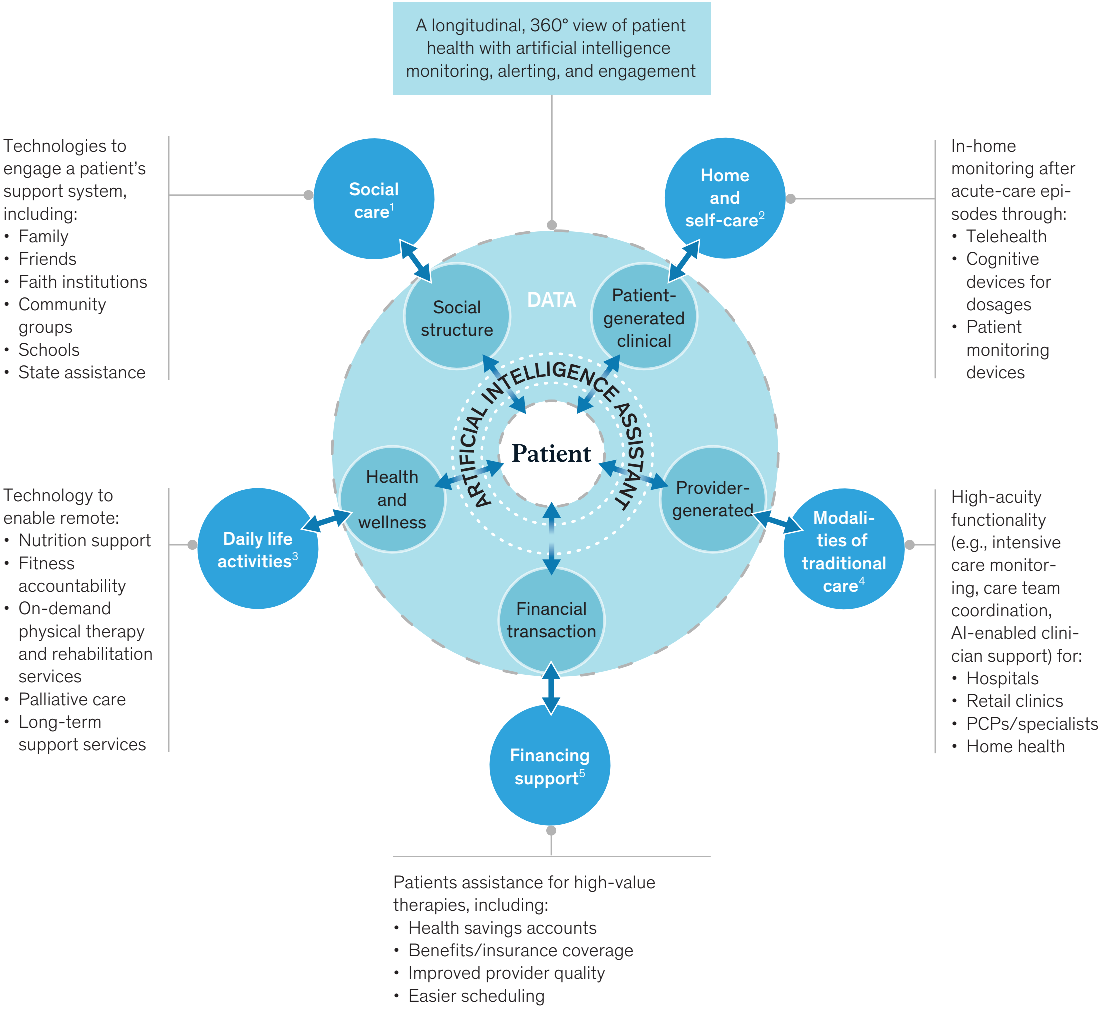
Attachment #10

New, personalized, and intuitive healthcare ecosystems. Perhaps the most significant change could be the creation of intuitive and personalized ecosystems of care centered around patients and their families, into which their community of medical and social caregivers would be integrated. Such ecosystems would make possible the delivery of the right type and amount of care, in the right setting, at the right time (Exhibit 5). The ecosystems could be enabled by a combination of:

— *holistic and longitudinal patient data sets* to integrate today's fragmented information from social systems, financial resources and

Exhibit 5

Intuitive ecosystems could enable access to the full continuum of care through technology-enabled modalities



A longitudinal, 360° view of patient health with artificial intelligence monitoring, alerting, and engagement

Technologies to engage a patient's support system, including:
- Family
- Friends
- Faith institutions
- Community groups
- Schools
- State assistance

In-home monitoring after acute-care episodes through:
- Telehealth
- Cognitive devices for dosages
- Patient monitoring devices

Technology to enable remote:
- Nutrition support
- Fitness accountability
- On-demand physical therapy and rehabilitation services
- Palliative care
- Long-term support services

High-acuity functionality (e.g., intensive care monitoring, care team coordination, AI-enabled clinician support) for:
- Hospitals
- Retail clinics
- PCPs/specialists
- Home health

Patients assistance for high-value therapies, including:
- Health savings accounts
- Benefits/insurance coverage
- Improved provider quality
- Easier scheduling

AI, artificial intelligence; PCP, primary care physician.

[1] Social care: Social and community networks related to a patient's holistic health.

[2] Home and self-care: Patient engagement, health-focused activities.

[3] Daily life activities: Patient actions enabling wellness, tangential to direct care delivery.

[4] Modalities of traditional care: Direct care administered by clinicians across evolving sites of care.

[5] Financing support: Operational and financial infrastructure of healthcare ecosystem.

Attachment #10

Sidebar

Considerations and cautions on this analysis

The range and pace of healthcare industry evolution remain to be determined; a variety of outcomes are possible by 2025, depending on the actions taken by various stakeholders. For instance, technology could simply make traditional care delivery systems marginally more efficient, or it could make possible radically new modes of care delivery focused around consumers (by enhancing both B2B and B2C healthcare delivery). Stakeholders must decide on their vision of the future if they are to effectively focus their strategies—for instance, by doubling down on aggregating the continuum of care or by orchestrating across technologies to meaningfully change how healthcare is delivered and managed.

It is worth remembering that experts have previously proclaimed that the healthcare industry is on the verge of technology disruption, yet little has materially changed. What's different today is the proliferation and liquidity of data, as well as the capabilities of data analytics and AI. In our estimates of value, we have analyzed only objective and measurable potential; however, the actual value delivered will depend on the path the healthcare industry takes, based on the economic and clinical decisions of individual stakeholders.

Additionally, to realize this objective value, several major barriers, such as the ones listed below, will likely need to be overcome:

— *the rate of technology adoption* and level of value creation, until now, has been much lower in healthcare than in other industries

— *the current healthcare regulatory structure* is complex, well-functioning standards for secure and full data interoperability are needed, and there is little transparency on costs and outcomes

— *the current reimbursement methodology* for providers, as well as pharmaceutical and device manufacturers, is still largely based on services rendered, not value delivered

— *fragmented sources of consumer data* (for example, medical records, self-monitoring data, social support inputs) are not yet broadly liberated nor integrated, a necessary change if technology is to effectively transform traditional modalities of care

If introduced in a haphazard or half-hearted way, the emerging innovations could increase, rather than reduce, the cost of care. Thus, stakeholders may need to carefully evaluate their strategies against their near- and longer-term ability to participate in the value-creating, integrated ecosystem of tomorrow.

systems, home-care and self-care monitoring, activities of daily life, and traditional modalities of care,

— *advanced analytics and AI personalization engines* to generate insights for patients and their community of caregivers,

— *continuum of care interaction models*, ranging from digital solutions to close-to-home services to traditional facilities, based on individual needs,

— *device-enabled, autonomous care* and cognitive engagement,

— *real-time refinement of individualized care solutions* and cognitive engagement through an AI-enabled interaction medium, and

Attachment #10

— *seamless integration of monitoring and care* from clinical caregivers, social and community structures, and family members.

We are aware that predictions of healthcare disruption have been made for decades. We want to be clear: we are not *predicting* that the US healthcare system will achieve net savings of $350 billion to $410 billion annually by 2025. Rather, we have reviewed the evidence, done the math, and identified use cases that *could* create $350 billion to $410 billion in technology-driven value annually by 2025. Realizing this value will require disruptors—incumbents and attackers alike—to understand the technologies available today, develop clear use cases with an evidence-based ROI, implement effective human change management strategies, and execute disciplined implementation plans. Stakeholders will need to make big bets on what role to play in this future, where to deploy capital, which capabilities to develop, what talent to attract, and how to drive such a transformation[37] in a world of exponential change. Some stakeholders will choose to maintain the status quo, but this approach will leave them at risk of either being left behind by disruptors or failing to capture part of the billions of dollars in net value.

[37] In our experience, driving such a transformation requires careful human change management and significant business model transformations.

Shubham Singhal (Shubham_Singhal@mckinsey.com), a senior partner in the Detroit office, is the global leader of McKinsey's Healthcare Practice. **Stephanie Carlton** (Stephanie_Carlton@mckinsey.com) is an expert associate partner in the Dallas office and co-leads our Center for US Health System Reform.

The authors would like to thank Neil Rao, Matt White, Marina Vigen, Mike Sturm, Shahed Al-Haque, Priyanka Sethy, Pieter Nel, and Walt Winslow for their contributions to this paper.

Editor: Ellen Rosen
For media inquiries, contact Nadine Mansour. For non-media inquiries, contact the authors.

Attachment #11

The new Apple-Google contact tracing tool finally seems useful

Public health authorities won't need to make their own apps in order to use Apple and Google's exposure notification tool.

By Sara Morrison Sep 1, 2020, 2:25pm EDT

The Apple-Google exposure notification tool is getting a major upgrade. The two companies just announced the debut of Exposure Notifications Express, which will enable their exposure notification tool to work without a public health agency needing to build or maintain an app around it. Now, states or public health authorities that don't have the resources or desire to build an app, but still want to take advantage of the tool, will be able to do so.

Streamlining the process of getting people to use this tool is a big deal. The Apple-Google tool is one of the most promising Big Tech attempts to help stop or contain the Covid-19 pandemic, but it has struggled to win over a lot of users. Without widespread adoption, contact tracing apps, including the ones that incorporate the Apple-Google technology, are basically useless: Studies have shown that at least 60 percent adoption is needed for a contact tracing app to be effective. But some experts say far less than that is needed when combined with human contact tracers.

"We estimate that a well-staffed manual contact tracing workforce combined with 15 percent uptake [in a contact tracing app] could reduce infections by 15 percent and deaths by 11 percent," Professor Cristophe Fraser in the department of health at Oxford University said in a statement.

So far, Maryland, Nevada, Virginia, and Washington, DC, have already signed on to use Exposure Notifications Express, while six states — Alabama, Arizona, North Dakota, Wyoming, Nevada, and Virginia — have apps that use the tool. While several other countries have apps that use the tool, the United States has left it to individual states to figure out their own contact tracing efforts, which have been less than enthusiastic. Although Apple and Google announced the exposure notification tool in April and launched it a month later, it wasn't until August that Virginia became the first state to release a contact tracing app that used the tool. Virginia told Recode that it spent nearly $230,000 to develop the app and $1.5 million to market it — money that came from the federal CARES Act. Nearly 500,000 Virginians have downloaded the app so far, which is a small portion of the state population of about 8.5 million people.

One huge upside to the new Exposure Notifications Express tool, however, is that states no longer have to spend the time or money developing their own apps. They may not have to do much marketing, either. In states or regions that have enabled Exposure Notifications Express, a prompt will pop up on phones with the latest version of Apple's or Android's operating system and alert the user that the tool is available to them. The user just taps the screen to enable it. For Apple users, that's all it takes to turn the tool on. Android users will then need to download an app that Google automatically generates for public health authorities. All public health authorities have to do is give Apple and Google some basic information and set up servers to host Bluetooth keys and exposure verification.

“As the next step in our work with public health authorities on Exposure Notifications, we are making it easier and faster for them to use the Exposure Notifications System without the need for them to build and maintain an app,” Apple and Google said in a statement. “Exposure Notifications Express provides another option for public health authorities to supplement their existing contact tracing operations with technology without compromising on the project’s core tenets of user privacy and security.”

Countries around the world have spent weeks trying various methods of contact tracing. The basic idea is that public health agencies can use contact tracing to notify people when they’ve potentially been exposed to the coronavirus so they can then quarantine and get tested accordingly. Contact tracing also helps track the virus’s spread, and that part is usually done manually, using human beings. Digital contact tracing tools, however, are designed to do this by using devices like smartphones to alert users when they’ve been close to a device tied to someone who’s potentially been exposed to the virus. The process of notifying people of potential exposure is where the Apple-Google exposure notification tool comes in handy.

The tool works by sending out and receiving anonymous Bluetooth “keys” from nearby phones that also have the tool enabled. If someone tests positive for the coronavirus, they can notify their public health authority, which will then send out alerts to any phones that were in proximity to the infected person’s phone. The system is designed to keep as much information as possible on individual phones and preserve user privacy. Very little information goes back to the public health authority, and users always have the option to opt in or out of the tool. Apple and Google have said that user privacy was a major consideration in their development of the tool, to encourage as many people to use it as possible. The two companies worked together on the project to allow the tool to work across their iOS and Android operating systems.

Contact tracing apps haven’t lived up to their potential so far, but Exposure Notifications Express should make it as easy as possible for public health authorities to implement them and people to enable them. Now we might get a chance to see what digital contact tracing apps can do — if it isn’t too late, six months into the pandemic, for them to make a difference.