General Committee Meeting
Thursday, November 19, 2020
3:00pm – 4:00pm

Zoom Link: https://zoom.us/j/94726187756?pwd=VnAzQTNiZFVWQUtWSjhsNVE3Q09IZz09
Meeting ID: 947 2618 7756
Password: 044829
Phone Number: 312 626 6799

1. Welcome and Introductions

2. Clear Health Pass

3. Regulatory Update — Attachment 1, 2
   a. ONC Interoperability Final Rule
   b. HIPAA Coordinated Care Proposed Rule
   c. FDA Communicating Cybersecurity Vulnerabilities Discussion Paper
   d. ONC USCDI Patient Matching Comments

4. Legislative Update — Attachment 3
   a. Senate Privacy Legislation

5. Monthly Privacy Round-Up — Attachment 4

6. Public Citizen Privacy and Digital Rights Report — Attachment 5

7. Next Steps for 2021

8. Articles of Interest — Attachment 6, 7, 8, 9

HHS Extends Compliance Dates for Information Blocking and Health IT Certification Requirements in 21st Century Cures Act Final Rule

Interim Final Rule with Comment Period Responds to COVID-19 Pandemic

Responding to public health threats posed by the coronavirus pandemic, today the U.S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health IT (ONC) released an interim final rule with comment period that extends the compliance dates and timeframes necessary to meet certain requirements related to information blocking and Conditions and Maintenance of Certification (CoC/MoC) requirements.

Released to the public on March 9, 2020, ONC's Cures Act Final Rule established exceptions to the 21st Century Cures Act's information blocking provision and adopted new health information technology (health IT) certification requirements to enhance patients' smartphone access to their health information at no cost through the use of application programming interfaces (APIs).

"We are hearing that while there is strong support for advancing patient access and clinician coordination through the provisions in the final rule, stakeholders also must manage the needs being experienced during the current pandemic," said Don Rucker, MD, national coordinator for health IT. "To be clear, ONC is *not* removing the requirements advancing patient access to their health information that are outlined in the Cures Act Final Rule. Rather, we are providing additional time to allow everyone in the health care ecosystem to focus on COVID-19 response."

In the Cures Act Final Rule, ONC set compliance dates and timeframes to meet certain requirements related to the information blocking and Conditions and Maintenance of Certification (CoC/MoC) requirements. In April 2020, ONC first responded to health IT stakeholders' concerns about the COVID-19 pandemic by exercising its enforcement discretion and providing three months after each initial date or timeline for all new requirements under the ONC Health IT Certification Program (Program).

The interim final rule issued today provides the health care ecosystem additional flexibility and time to effectively respond to the public health threats posed by the spread of COVID-19. It extends the Program compliance dates beyond those identified in the April 21, 2020, enforcement discretion announcement and establishes new future applicability dates for information blocking provisions. The interim final rule also adopts updated standards and makes technical corrections and clarifications to the ONC Cures Act Final Rule.

New Applicability and Compliance Dates/Timeframes & Corresponding Provisions

April 5, 2021	December 31, 2022	One Calendar Year Extension
• Information blocking provisions (45 CFR Part 171) • Information Blocking CoC/MoC requirements (§ 170.401) • Assurances CoC/MoC requirements (§ 170.402, except for § 170.402(b)(2) as it relates to § 170.315(b)(10)) • API CoC/MoC requirement (§ 170.404(b)(4)) - compliance for current API criteria • Communications CoC/MoC requirements (§ 170.403) (except for § 170.403(b)(1) – where we removed the notice requirement for 2020)	• 2015 Edition health IT certification criteria updates (except for § 170.315(b)(10) – EHI export, which is extended until December 31, 2023) • New standardized API functionality (§ 170.315(g)(10))	• Submission of initial attestations (§ 170.406) • Submission of initial plans and results of real world testing (§ 170.405(b)(1) and (2))

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

Attachment #2

Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework

DISCUSSION PAPER AND REQUEST FOR FEEDBACK

PATIENT ENGAGEMENT ADVISORY COMMITTEE

October 2020

Contents

Background

The U.S Food and Drug Administration's (FDA's) Center for Devices and Radiological Health (CDRH) remains committed to its mission to promote and protect the public health, including the safe and effective use of medical devices that are connected to the Internet, hospital networks, and other medical devices (hereafter referred to as "connected medical devices"). These medical devices range from sensor-based technologies such as wearables, to implantable medical devices, such as pacemakers. The increased use of connected medical devices in the United States has led to an increase in cybersecurity vulnerabilities. The FDA is at the forefront of helping mitigate cybersecurity issues related to the use of connected medical devices. Currently, the FDA's safety communications fall into two main categories: device-specific information and underlying technology issues. The FDA tailors its communications depending on the specific audiences (such as patients, healthcare providers, and industry) and the communication type (such as safety or educational communications). The FDA also tailors its communications based on the urgency of the issue and the public health impact. The FDA acts promptly to communicate on cybersecurity vulnerabilities with the public to ensure they are aware of these issues and have the information they need to take appropriate action. Clear, actionable communication is one way to help protect and promote public health, and helps ensure that patients, who depend on their medical devices, stay informed and protected.

The Patient Engagement Advisory Committee (PEAC or the Committee) provides advice to the Commissioner or their designee on complex, scientific issues relating to medical devices, the regulation of medical devices, and their use by patients. The PEAC may consider topics such as Agency guidance and policies, clinical trial or registry design, patient preference study design, benefit-risk determinations, device labeling, unmet clinical needs, available alternatives, patient-reported outcomes, and device-related quality of life or health status issues. The Committee provides relevant skills and perspectives, in order to improve communication of benefits, risks, clinical outcomes, and increase integration of patient perspectives into the regulatory process for medical devices.[1]

During the PEAC meeting on September 10, 2019, the members expressed the importance of clearly and consistently communicating about cybersecurity vulnerabilities, as well as clearly identifying when patients need to take an action to mitigate potential harms. These findings are shared in the Summary

[1] More information about PEAC can be found at: https://www.fda.gov/AdvisoryCommittees/CommitteesMeetingMaterials/PatientEngagementAdvisoryCommittee/default.htm

of the Patient Engagement Advisory Committee document. The FDA's Internal Message Testing Network (for which participants serve as a proxy for the public) also reviewed four cybersecurity messages created by the FDA and manufacturers. This review provided insights on how the FDA and potentially other stakeholders in the field of cybersecurity vulnerability communications could tailor approaches for communicating about cybersecurity vulnerabilities with patients and caregivers. The feedback from these stakeholders is the foundation for the development of this document.

Goals

The FDA is holding its next PEAC meeting on October 22, 2020 and has developed this discussion paper to provide potential best practices and elements to consider when developing a cybersecurity communication framework. These elements include:

- interpretability;
- discussing risks and benefits;
- acknowledging and explaining the unknown;
- availability and findability of information;
- structure of the communication material; and
- outreach and distribution vehicles.

The FDA seeks further input from patients, patient advocacy organizations, the medical device industry, clinical researchers, and others on this topic. The FDA intends to use this feedback to inform future efforts designed to improve cybersecurity safety communications, including the potential development of a cybersecurity communications framework. In particular, the FDA seeks further comment from the public on the following questions:

1. Are the elements outlined as part of the considerations for a framework the most appropriate and relevant for effective communication about cybersecurity vulnerabilities with patients and the public?

2. Are there any elements that are missing, or that could be strengthened or clarified to help develop a useful framework?

Important Elements to Consider

The feedback received at the 2019 PEAC Meeting and through the FDA's Internal Message Testing Network highlighted important elements to include in the development of safety communications for cybersecurity vulnerabilities. Such elements include interpretability, discussing risks and benefits, acknowledging and explaining the unknown, availability and findability of the information. This document expounds on these elements, which comprise the considerations that may inform a potential future communications framework for cybersecurity vulnerabilities. These elements are discussed below with an example of how these elements might be applied (**Appendix**).

Interpretability: Make it Easy for People to Read and Understand

When developing safety communications, it is important to consider the messenger's need to communicate the messages in clear and plain language with the audience's need to receive and understand the message conveyed. Throughout this document, messengers may include the FDA, other federal agencies, and industry; the audience may include patients and caregivers. Several factors, such as timeliness, relevance, simplicity, and readability for diverse audiences are key for patients and caregivers to read and understand the safety communications.

Keep it Timely

Whenever possible, communicate with patients and caregivers as early as possible, especially if the cybersecurity vulnerability presents a serious threat. Early access to serious cybersecurity vulnerability information may provide assurance to patients and empower them to take early action to avoid any potentially harmful consequences to their health. Furthermore, early access to this information may also help build trust with patients and the public.

Keep it Relevant

Patients and caregivers have indicated that communicating risk and urgency are important to them. Clearly explaining the risks near the top of the safety communication and stating the urgency of the risk is one way to help emphasize critical information to the audience. It is also important to have a call to action (i.e., clear actions that patients and caregivers can take) so that patients and caregivers know what steps to take to mitigate those risks if possible. In some cases, it may not be possible for patients to mitigate risks, as an update to their device may not yet exist, or they may need to wait for the medical device manufacturer, healthcare provider, or other party to take some action first. In these cases, it may be helpful to clearly outline what patients can and cannot do. The communication should

provide clear and concise instructions for recommended actions and focus on what patients and caregivers should do.

One way to help ensure communications are relevant is to conduct message testing with target audiences. Organizations may want to consider having patient advisory boards that could assist with message refinement.

Keep it Simple

To best reach your target audience, it is helpful to communicate about cybersecurity vulnerabilities in the simplest way possible. Using terminology that your target audience understands is a best practice in communications, and pilot testing the communication with your audience can help you better assess what they do and do not understand (Centers for Disease Control and Prevention, 2019). When developing safety communications, it is helpful to avoid the use of technical language and jargon and avoid acronyms or, if acronyms are necessary, spell them out when they first appear. If some degree of technical jargon is necessary, it can be helpful to provide plain language explanations of the jargon in the same sentence in which the terminology is introduced or immediately following. One form of technical jargon may include the name of the cybersecurity vulnerability. The FDA's Internal Message Testing Network found that the target audience confused the name of the vulnerability with the name of the device. It would help patients if the communications clearly explain the difference between the name of the vulnerability and any affected medical devices.

Keep it Readable for Diverse Audiences

While keeping it simple will help enable all audiences to better understand the communication, it is also important to ensure that the information is available to diverse readers in their preferred language. Providing translation services for relevant languages may increase the number of people who read and understand the communication. For instance, if a specific issue targets elderly Hispanic and Latinx patients that may primarily speak Spanish, it may help reach the target audience if the safety communication was available in Spanish. Language translation is not simply writing text in another language, but also includes considering the cultural nuances of speech when crafting the message. Due to the nuances of cybersecurity communications and regulatory language, using machine translations is not a best practice, as these translators may not capture the subtleties of the language and may misinform or confuse the reader.

Discuss Risks and Benefits

During the PEAC meeting, the Committee stated that it was important for messengers to convey a balanced discussion between the risks and benefits when the probability of cybersecurity exploitation remains unknown. In particular, the Committee recommended a "balanced discussion between risk and benefits, highlighting the benefits especially if it is a lifesaving device" (Summary of Patient Engagement Advisory Committee, 2019). When discussing cybersecurity vulnerabilities, if there are risks associated with mitigations, it is important to discuss both the risks and benefits of actions related to addressing the specific vulnerability. The goal is to help provide patients and caregivers information about their options when deciding to act or not act on a specific issue or call to action.

Acknowledge and Explain the Unknown

If something is not known at the time of the communication, consider acknowledging and explaining to the audience the unknown information so that this is not perceived as an omission (intentional or unintentional) or an oversight. This will also help the reader have confidence that the information is accurate and trustworthy. For instance, if there is a vulnerability detected for a device, but that device has no means by which to detect whether the vulnerability has been exploited, it is important to note that there are "no known exploits at this time," rather than "no exploits," as it would be impossible to state there were no exploits with certainty.

Availability and Findability: Make it Easy for Patients to Find and Use

As noted in the Summary of the Patient Engagement Advisory Committee (PEAC) from September 10, 2019 (Summary of Patient Engagement Advisory Committee, 2019):

> "The Committee generally believes that knowledge does not necessarily confer responsibility and that the burden should not be put on the patient to find the information pertaining to risks or threats associated with their device(s). **FDA should make sure that burden is on industry to communicate the risk and not pushed back on patient to find it."** (emphasis added)

The FDA and industry share responsibility for communicating about cybersecurity risks in medical devices to patients and caregivers in a manner that is easy to find. The elements below expound upon the best practices of availability and findability, which include more considerations for a potential future communications framework for cybersecurity.

Make Communications Easy to Find in Online Searches

Numerous studies have shown that patients use internet searches to find health information. (Diaz, et al., 2002) (Madrigal & Escoffery, 2019). Online search engines drive a large proportion of visits to the FDA's safety communications. In addition, patients and caregivers may hear about cybersecurity vulnerabilities before receiving an alert from a device manufacturer and may attempt to search for more information using an internet search.

Safety communications on cybersecurity risks are more easily found if they incorporate best practices in search engine optimization (SEO) techniques, such as:

- including the name of the manufacturer and device name (or device category name) in the title of the communication, if the cybersecurity vulnerability is specific to a medical device or group of medical devices;
- including other important keywords that patients may search for near the beginning of the title, such as the name of the cybersecurity vulnerability; and
- incorporating important keywords in the content itself, including the list of specific medical devices, as well as the associated diseases or conditions.

Feedback from the FDA's Internal Message Testing Network indicated a patient preference for including medical device names in the title of the communication. This feedback also indicated that including the name of the vulnerability in the title was often confused with the medical device name. For findability purposes, it is important to include the name of the cybersecurity vulnerability in the title. Hence, a clear presentation of how names are used is critical to patient and public understanding and identification.

Make Communications Easy to View on Mobile Devices

According to the Pew Research Center (Mobile Fact Sheet, 2019), the vast majority of adults in the United States (96 percent) own a smartphone of some kind, and 37 percent of U.S. adults surveyed (Anderson, 2019) mostly use a smartphone when accessing the Internet. For certain groups, such as younger adults and adults without a broadband connection at home, that percentage is even higher. Metrics for mobile access of the FDA's safety communications show that, depending on the topic, most visitors are using mobile devices to read the information (Unpublished Data, 2020).

For these reasons, safety communications on cybersecurity risks may be more effective if they incorporate best practices for mobile-friendly content. The FDA adopted a mobile-friendly, responsive design approach to its web content in 2013. Some mobile-friendly best practices include:

- Chunking content for easy scanning by using sub-headers, lists, bullets, simple tables, and other formatting techniques;
- Using brief paragraphs and short titles that are easier to read on a smaller screen; and
- Following the plain language principles described above in the *Interpretability* section.

Mobile-friendly designs and writing techniques also enhance findability, since search engines rank mobile-friendly content higher in search results pages (Uzialko, 2020).

In addition, making communications accessible for individuals with disabilities will enable these audiences to better access cybersecurity vulnerability communications. All federal agencies must comply with Section 508 of the Rehabilitation Act, which "require[s] federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities" (IT Accessibility Laws and Policies, 2020).

Communication Structure

Information hierarchy is essential to safety communication structure. It is important for patients and caregivers to quickly find information relevant to them. Thus, it is important for safety communications to lead with the main message and recommendations for patients and caregivers.

Good organization is also an important factor when constructing safety communications. Consider your audience and put clear and succinct messages that are most relevant to patients and caregivers at the top, near the beginning of the safety communication. The FDA's Internal Message Testing Network showed a preference for communications that are short. Include information about specific diseases or affected medical devices, as applicable, at the top of the communication.

Additionally, providing visual cues, such as simple tables, call out boxes, *italics*, and **bolded text**, among others, to draw the reader's attention to the main message can be beneficial to craft a message that is compelling and palatable to lay audiences. For instance, grouping information about one disease or device in the same section (such as diabetes or pacemakers) could help readers better identify and understand the information.

Outreach and Distribution Vehicles

As with any important communication issues, having an outreach plan and developing appropriate communication channels help aid the comprehensive dissemination of information about safety communications, including cybersecurity vulnerabilities. Depending on the type of vulnerability, the messenger may need to conduct outreach with partner organizations to help inform the target audience. Different types of vulnerabilities and audiences may need different approaches, so it is important to consider which combination of distribution vehicles could be used to maximize outreach.

Outreach Plan

It is important for the outreach plan to consider the target audience, key messages, and distribution vehicles intended to reach the target audiences. When developing an outreach plan, consider the must-reach audience for the communication material and determine how best to assure they receive the message. These considerations may include age, race, ethnicity, language, geography, disease, device use, or any other identifying feature that could help inform approaches that might be effective at having the greatest impact. Advance planning for these types of communications is important, as is reaching the target audiences. Given the need to communicate quickly, it may be advantageous to develop ongoing relationships with outreach partners prior to an incident occurring. This planning may help ensure that when the time comes, these relationships are in place for rapid communication deployment. Creating a template for these types of communications may also enable faster communications.

Distribution Vehicles

There are many possible distribution vehicles to reach different audiences. Using a combination of different distribution vehicles may lead to the greatest dissemination of the communication materials. For example, if the affected device is specifically used for a condition impacting many African Americans and the Hispanic and Latinx population, then the distribution vehicles may need to be augmented to assure outreach to these populations. Just as language may be tailored for the target audience, and communications may be translated based on target audience, distribution vehicles may be tailored for the target audience. Each communication plan may consider the unique needs of the audience and tailor distribution vehicles based on how to best reach those patients.

The list below, while not comprehensive, reflects the distribution vehicles mentioned during the FDA's Internal Message Testing efforts and the 2019 PEAC meeting. It also reflects participants' thoughts on the utility and reliability of such vehicles.

- **Email and patient listservs** – Direct emails to patients or use a listserv (for instance to consumer and patients' groups or state, local, and territorial governments) to communicate with patients and caregivers is also an effective way to reach out your target audience. Participants found emails and listservs to be a reliable way of receiving information.
- **Text messages** – The use of a company-based text program has been used to reach target audiences to deliver safety information. Text message programs have been used for public health interventions, can be relatively inexpensive, and can be a direct channel to reach the target audience. As patients increasingly rely on cell phones for communication, text messaging can be an instantaneous communication vehicle that patients can read at their convenience (Wagner, 2019). Participants found text messages to be a reliable way of receiving information.
- **Social Media** –Recent research has shown that information quality and authority is a concern when people consider using health information from social media but that credibility may vary by type of social media channel (Zhao & Zhang, 2017). Although the use of social media is widespread, some of the participants indicated that they did not consider social media to be a reliable source of information as it may be perceived as spam (unsolicited digital communication sent out in bulk).
- **Television** – Participants also considered television to be a reliable source of information. Because this can be an expensive vehicle to deliver information, organizations could consider whether this is an appropriate and feasible vehicle for them.
- **Websites** – Government and private industry use their own websites to disseminate safety information. Whether organizations use safety alerts or other media vehicles (such as a press release or an in brief), they try to maximize this channel to deliver safety information. Although participants were not asked directly about their preferences for websites, the other distribution vehicles typically direct patients to websites to find more information. When applying best practices described above, websites can be an effective tool for communication.

Conclusion

Communicating about medical device safety is an important part of the FDA's work to ensure patient safety and the overall safety and effectiveness of medical devices. As the use of connected medical devices increases and cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful (U.S. Food & Drug Administration, 2018), it is increasingly

important for the FDA, industry, and other stakeholders to improve on cybersecurity safety communications. These considerations for a framework are a critical step to begin this improvement.

It is essential that communications be available, easy to find, and easy to understand. Additionally, it is critical for them to be timely, relevant, simple, and readable for a diverse audience, discuss the risks and benefits, and acknowledge any unknown information. Information about cybersecurity vulnerabilities is vital to share with patients and caregivers to help them make informed decisions about their health and their medical devices.

Appendix: Sample Cybersecurity Vulnerability Safety Communication

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

Your Brand X Insulin Pump May Be Affected by X Cybersecurity Risk

*Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. These are **cybersecurity risks**.*

Contact your health care provider right away if you think your Brand X insulin pump settings or insulin delivery changed unexpectedly.

An unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby **Brand X** insulin pump. This unauthorized person could change the pump's settings to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar (hyperglycemia) and diabetic ketoacidosis.

The FDA recommends people who have affected **Brand X** insulin pumps update the software on their devices to protect them from these risks.

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

The FDA recommends people who have affected **Brand X** insulin pumps update the software on their medical devices to protect them from these risks.

> At this time, the FDA has not received any confirmed reports of unauthorized persons changing settings or controlling insulin delivery to **Brand X** insulin pumps.

Check to See if Your Insulin Pump Is Affected by X Cybersecurity Risk

Certain **Brand X** insulin pumps may be affected by this cybersecurity risk. People who have diabetes and use these models should update their insulin pump to the latest version of the device software to protect against these potential risks.

Read the **Brand X** Letter to Patients to learn how to identify your pump's software version.

If You Believe Your Insulin Pump May Be Affected by X Cybersecurity Risk:

- Talk to your health care provider if you believe your treatment has been affected.
- Update the software of your insulin pump to ensure more cybersecurity protection.
- If you have questions about updating your pump software, call **Brand X** at 1.800.555.1212 or email updatepump@BrandX.com or visit www.BrandX.com.
- Follow the steps listed below in "**Everyone With an Insulin Pump Should Take the Following Steps to Help Prevent the Risk of a Cybersecurity Attack**."

Get Medical Help Right Away if You:

- Have symptoms of severe hypoglycemia (such as excessive sweating, feeling very tired, dizzy and weak, being pale, and a sudden feeling of hunger).
- Have symptoms of diabetic ketoacidosis (such as excessive thirst, frequent urination, nausea and vomiting, feeling very tired and weak, shortness of breath).
- Think your insulin pump settings or insulin delivery changed unexpectedly.

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

Everyone With an Insulin Pump Should Take the Following Steps to Help Prevent the Risk of a Cybersecurity Attack:

- Keep your insulin pump and the devices connected to your pump within your control at all times.
- Do not share your pump serial number.
- Be attentive to pump notifications, alarms, and alerts.
- Monitor your blood glucose levels closely and act appropriately.
- Immediately cancel any unintended boluses.
- Connect your **Brand X** insulin pump to other **Brand X** devices and software only.
- Disconnect the USB device from your computer when you are not using it to download data from your pump.

Download image

Report Problems with Your Insulin Pump

Report any problems you have with your insulin pump to the FDA through the MedWatch Voluntary Reporting Form.

More Information

- **Brand X's** Letter to Patients.
- Cybersecurity: The FDA's webpage about cybersecurity risks and medical devices

The FDA will provide updates as new information becomes available.

Questions?

If you have questions, email the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV or call 800-638-2041 or 301-796-7100.

Comparison of Federal Privacy Bills

	SAFE DATA ACT (WICKER BILL)		
	Provisions	**Alignment with HIPAA**	**Practical Implications**
Covered Entity (CE)	A CE is any entity subject to FTC Act as well as a common carrier and non-profit that: (1) collects, processes, or transfers covered data; and (2) determines the purposes and means of such collection, processing, or transfer.	Would apply to HIPAA covered entities(CEs) and business associates (BAs) with respect to activities <u>not</u> subject to HIPAA	HIPAA CEs and BAs would need to determine which activities, if any, involving covered data fall outside of HIPAA that fall within Wicker bill (given that Wicker bill does not apply to employee data). Wicker bill would arguably apply to (1) non-health components of hybrid entities; and (2) PHI used pursuant to a HIPAA authorization on behalf of non-HIPAA entities (e.g., pharmaceutical manufacturers).
Covered Data	Information that identifies or is linked or reasonably linkable to an individual or a device[1] that is linked or reasonably linkable to an individual. <u>Exclusions</u> (1) aggregated data, (2) de-identified data[2], (3) employee data and (4) publicly available information.	Uses a different standard/definition for de-identified data.	Data de-identified under HIPAA but that does not meet the standard under the Wicker bill (e.g., recipients not legally bound to not attempt to re-identify the data) would fall under Wicker bill. To avoid this, HIPAA entities would need to ensure that

[1] Data 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 the individual or device.

[2] "De-identified data" means information 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 or the device; (iii) is subject to a public commitment by the covered entity to refrain from attempting to use the information to identify any individual or device and to adopt technical and organizational measures to ensure that the information is not linked to any individual or device; and (iv) is not disclosed to any other party unless the recipient is legally bound to not use the data to identify any individual or device, and any onward disclosures are subject to the same legally binding agreement.

			they de-identify PHI in a manner that meets the standards of both HIPAA and Wicker bill.
Privacy Policy	A CE must provide a privacy policy before point of collection of covered data and available to the public in a clear and conspicuous manner that includes: (1) the identity and the contact information of the CE and the identity of any affiliate to whom covered data may be transferred; (2) the categories of covered data the CE collects; (3) the purposes for which each category of covered data is collected; (4) the categories of recipients to whom the CE transfers covered data, and the purposes of the transfers; (5) a general description of the CE's data retention practices and the purposes for the retention; (6) how individuals can exercise their rights; (7) a general description of the CE's data security practices; (8) the effective date of the privacy policy. The policy must be made available in the language the CE provides its products and services. If the CE makes any material changes to the policy it must notify affected individuals before further processing or transferring previously collected data and give them an opportunity to withdraw consent to further processing or transfer of the data. Where possible, notification must be made directly, taking into account available technologies and the nature of the relationship with the individual.	More granular than HIPAA Notice of Privacy Practices (NOPP) in that it requires identity of any affiliate with whom covered data is shared, categories of covered data collected, categories of recipients, description of data retention practices and purposes, and a description of data security practices. No language requirements for NOPP. No requirement for HIPAA CEs to allow individuals to opt out of further processing or transfer of their previously collected data when it makes material changes to its NOPP	HIPAA CEs that conduct activities falling outside of HIPAA that involve covered data would need to create separate privacy policies for this covered data, provide the policy in accordance with different time frames, and allow opt out with respect to previously collected data when they make material changes to the policy. This would in turn required CEs to have a means of keeping track of when covered data was collected and the privacy policy applicable at that time.
Individual Rights	Individuals have the following rights:	HIPAA does not include: (1) right to know categories of third	HIPAA CEs that conduct activities falling outside of

	(1) access (including right to list of categories of third parties and service providers with whom the data is shared and the purpose); (2) correction of material inaccuracies or incomplete data (and to notify service providers and third parties with whom the data has been shared; (3) deletion or de-identification (and to notify service providers and third parties to whom the data has been transferred of this request unless the data was transferred at the request of the individual; and (4) portability i.e., to the extent technically feasible, provide the data in a portable, structured, machine readable format not subject to licensing restrictions. A CE may not deny products or services to an individual for exercising their rights (unless the exercise of the rights precludes this), but may offer different pricing or functionality. <u>Exceptions</u> A CE may deny a request that: (1) requires retention of the data solely for purpose of fulfilling the request; (2) is impossible or demonstrably impracticable to comply with; (3) require the CE to reidentify covered data that has been deidentified; (4) result in the release of trade secrets or other proprietary or confidential data or business practices; (4) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to detect, or	parties and service providers with whom data is shared; (2) right to delete or de-identification; or (3) portability, although it does have requirements to provide PHI in an electronic designated record set electronically and otherwise provide the PHI in the format requested if readily producible in that format. CEs may not retaliate against individuals for filing a complaint that their HIPAA rights have been violated. HIPAA bases for denial of rights are generally more limited, mostly related to psychotherapy notes, records created in anticipation of litigation, records created in the course of research or where providing the records would create a risk to the health or safety of the individual or others.	HIPAA that involve covered data would need to put in place policies and procedures to allow individuals to exercise new rights (with different requirements e.g., different bases for denial of requests) with respect to that covered data.

	investigate malicious or unlawful activity, or enforce contracts;(5) require disproportionate effort; (6) compromise the privacy, security, or rights of others' covered data, (7) be excessive or abusive to another individual; or (8) violate federal or state law or the rights and freedoms of others.		
Consent	A CE must obtain "affirmative express consent"[3] before processing or transferring sensitive covered data.[4] Minors. A CE may 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 CE entity has actual knowledge that the individual is between 13 and 16 years of age. Right to Opt Out. A CE must provide an individual with the ability to opt out of the collection,	No consent required to use or disclose PHI (including that of minors) for a CE's treatment, payment or health care operations, as well as public health, health oversight, judicial proceedings, law enforcement and limited other purposes. Written authorization required to use or disclose PHI for marketing purposes, research (unless an IRB or privacy board determines the research involves	HIPAA CEs that conduct activities falling outside of HIPAA that involve covered data would need to obtain affirmative express consent to use, transfer or process that data, unless the purpose falls within an exception. For example, if PHI used pursuant to a HIPAA authorization on behalf of a non-HIPAA entity falls under the Wicker bill, in addition to obtaining a HIPAA authorization

[3] "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." As such, it does not appear to require written consent.

[4] "Sensitive covered data" means: (i) A unique, government-issued identifier; (ii) covered data that describes or reveals an individual's diagnosis or treatment; (iii) A financial account number, debit card number, credit card number, or any security code or password (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 CE is the intended recipient; (viii) Account log-in credentials in combination with a password or security Q&A 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; (x) covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation; (xi) covered data about the online activities of an individual that addresses or reveals another category of covered data; (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.

	processing, or transfer of covered data before its collection, processing, or transfer. Affirmative express consent may not be inferred from an individual's inaction or continued use of a product or service. A CE must provide an individual with a clear and conspicuous means to withdraw affirmative express consent. <u>Exceptions</u>: Consent not required for the following purposes provided that the collection, processing, or transfer is reasonably necessary, proportionate, and limited to the purpose: (1) to complete a transaction or fulfill an order specifically requested by an individual; (2) to perform internal system maintenance; (3) to respond to a security incident or maintain security; (4) to protect against malicious, deceptive, fraudulent, or illegal activity; (5) to comply with a legal obligation, defend a legal claim or as specifically permitted or authorized by law; (6) to comply with a legal proceedings or a regulatory inquiry; (7) to cooperate with an Executive agency or a law enforcement official concerning conduct that may violate the law, or pose a threat to public safety or national security; (8) to address risks to the safety of an individual or groups; (9) to effectuate a product recall; (10) to conduct research that is in the public interest and meets certain conditions; (11) to transfer covered data to a SP; and (12) for a purpose identified by the FTC in regulations.	minimal risk to individual privacy) and generally to obtain remuneration in exchange for PHI. No requirement to allow opt-out of collecting, processing or transferring PHI generally. Individuals must be permitted to revoke their authorizations. Exceptions to consent in Wicker bill roughly correspond to purposes for which PHI may be used without an authorization under HIPAA, except Wicker bill would allow use of covered data for research that is in the public interest without consent.	to use the covered data, HIPAA entities would need to obtain the individual's prior express consent to do so for certain purposes (and this consent could not be combined with the HIPAA authorization, otherwise it would invalidate the HIPAA authorization).

Data Minimization	A CE may not collect, process, or transfer covered data beyond what is reasonably necessary, proportionate. Not later than 1 year after enactment, the FTC will issue guidelines on best practices to minimize the collection, processing and transfer of covered data.	HIPAA requires compliance with minimum necessary, subject to certain exceptions, including treatment.	
Service Provider (SP)	A SP: (1) may not process SP data[5] for any purpose other than as directed by the CE; (2) may not transfer SP data to a third party for any purpose other than as directed by the CE without the affirmative express consent of the individual; (3) at the direction of the CE, must delete or deidentify the SP data as soon as practicable after completing the service or function for which the data was provided. A SP is exempt from the individual rights requirements but must, to the extent practicable, assist the CE in fulfilling requests by individuals to exercise their rights and must, upon notice by the CE of receipt of a verified request, delete, de-identify or correct SP data. A SP is exempt from the consent and data minimization requirements.	HIPAA requires CE to enter into written agreements with BAs that specify the permitted purposes for which PHI may be used and disclosed. PHI must be returned or destroyed upon termination of BA relationship if feasible. BAs must comply with HIPAA individual right requests, either directly or by providing the data to the CE to respond. BAs must comply with minimum necessary requirements and generally may not use or disclose PHI for purposes for which the CE may not use or disclose it.	HIPAA CEs that conduct activities falling outside of HIPAA that involve covered data would need to enter into agreements with SPs that meet the Wicker bill requirements and exercise due diligence in choosing SPs. These contract requirements would be in addition to any business associate agreements entered into with the same SPs involving activities subject to HIPAA.

[5] Service provider data is 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, the covered entity.

	A CE must exercise due diligence before selecting a SP to ensure compliance with the above requirements.	No specific requirement to exercise due diligence in selecting BAs, but CEs are responsible for Breaches by BAs and may be liable for violations by BAs.	
Third Parties	A third party may not process third party data[6] for a purpose inconsistent with the reasonable expectation of the individual. The third party may reasonably rely on representations made by the CE as to the reasonable expectations of the individual, provided it conducts reasonable due diligence on the representations of the CE and finds them credible. A third party is exempt from the consent and data minimization requirements. If a CE enters bankruptcy proceedings requiring the transfer of covered data to a third party, it must notify affected individuals (including the name and privacy policies and practices of the third party) and give them the opportunity to withdraw their consent or request that their data be deleted or de-identified. A CE must exercise due diligence before transferring covered data to a third party to ensure compliance with the above requirements	HIPAA does not regulate PHI in the hands of third parties that are not CEs or BAs.	HIPAA CEs that conduct activities falling outside of HIPAA that involve covered data would need to implement processes to exercise "due diligence" before sharing that covered data with third parties. Special requirements applicable to HIPAA CEs entering bankruptcy proceedings.
Large Data Holders	CEs that are large data holders[7] must, within 1 year of enactment or becoming a large data holder,	HIPAA does not require a privacy assessment by any CEs.	HIPAA CEs that conduct activities falling outside of

[6] "Third party data" means covered data that has been transferred to a third party by a covered entity.

[7] A "large data holder" means a covered entity that in the most recent calendar year either (1) processed the covered

	conduct a privacy impact assessment of their processing activities involving covered data that present a heightened risk of harm to individuals. Every 2 years thereafter they must conduct privacy assessments of the extent to which their privacy practices are consistent with their privacy policies, and that their privacy settings are accessible, consistent with individual expectations and give individuals adequate control over their covered data.	But all CEs and BAs are required to do a risk analysis and implement a risk mitigation plan.	HIPAA that involve covered data and that qualify as large data holders would need to conduct regular privacy assessments of their activities involving covered data
Small Business Exception	CEs that are small businesses are exempt from the requirement to provide individual rights, data minimization and requirement to designate a privacy and security officer. A small business is an entity that over the preceding 3 years: (1) had average annual gross revenues that did not exceed $50 million; (2) on average processed covered data of less than 1 million individuals; (3) never employed more than 500 individuals at one time; and (4) derived less than 50% of its revenue from transferring covered data.	HIPAA has no small business exception.	
Discrimination	If the FTC obtains information that a CE may have processed or transferred covered data in violation of federal anti-discrimination laws, it must send the information to the appropriate executive or state agency to initiate proceedings. The FTC must submit an annual report to Congress on the types of data sent to executive or state agencies and how it relates to anti-discrimination laws.	No requirement for OCR to send information concerning possible violations of ant-discrimination laws by CEs to appropriate regulatory agencies.	

data of more than 8 million individuals; or (B) processed the sensitive covered data of more than 300,000 individuals or devices that are linked or reasonably linkable to an individual (excluding processing of log-in information to allow an individual to access an account administered by the covered entity).

	The FTC must conduct a study and publish a report on this study on the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws, and may issue guidance to help CE's avoid using discriminatory algorithms.		
Security	A CE must implement and maintain reasonable administrative, technical, and physical data security policies and practices. These policies and practices must be appropriate to the size and complexity of the CE, the nature and scope of its covered data collection or processing, the volume and nature of the covered data, and the cost of available tools to improve security and reduce vulnerabilities. The FTC must issue guidance within 1 year of enactment on how to identify vulnerabilities to covered data, manage access rights, use SPs and take reasonable preventive and corrective measures to address vulnerabilities, and detect and respond to cybersecurity incidents. A CE that is required to comply with, and is in compliance with, the information security provisions of Gramm-Leach Bliley or the HITECH Acts will be deemed to be in compliance with the above requirements.	HIPAA requires administrative, technical and physical safeguards, policies and procedures. Requirements are technology-neutral and scalable to the size of the entity.	Since compliance with HIPAA would be deemed compliance with Wicker bill requirements, no additional responsibilities for HIPAA CEs or BAs.
Other Provisions	Filter bubble Transparency. Requires covered internet platforms that use an "opaque algorithm"[8] to: (1) provide notice to users that they do so to select the content the user sees based on user-	Not addressed in HIPAA.	

[8] An "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 that purpose.

	specific data, and (2) make available a version of the platform that uses an input-transparent algorithm (i.e., one not based on user-specific data) and enables users to easily switch between the two version of the platform.[9] Manipulation of User Interfaces. Makes it unlawful for a large online operator[10] (1) to design, modify, or manipulate a user interface for purposes of impairing the user's decision-making or choice to obtain consent or user data; (2) to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies unless it obtains the informed consent of each user involved; or (3) to design, modify, or manipulate a user interface on a website or online service directed at children under the age of 13 in order to cultivate compulsive usage. Requires large online operators to disclose to users and the public certain information regarding experiments or studies conducted based on user activities or data and have any such experiments approved by an Independent Review Board. Provides safe harbor for large online operators acting in accordance with a registered professional standards body that meets certain requirements.		

[9] This requirement does not apply to a downstream provider of a search engine that employs fewer than 1000 individuals and search engine uses an index of web pages on the internet to which the provider received access under a search syndication contract.

[10] A "Large online operator" is any person that provides online services that have more than 100 million authenticated users in any 30-day period and is subject to the jurisdiction of the FTC.

Corporate Accountability	A CE must designate a data privacy and data security officer. A CE must maintain internal controls and reporting structures to ensure that appropriate senior management officials are involved in assessing risks and making decisions that implicate compliance with the Act. In assessing penalties, the FTC will consider whether a CE retaliated against a whistleblower.	HIPAA requires CEs to have a privacy and security officer, and BAs to have a security officer. No specific requirements regarding roles or responsibilities of senior management.	HIPAA CEs that conduct activities falling outside of HIPAA that involve covered data would need to ensure that internal controls and reporting structures comply with Wicker bill requirements.
Enforcement	By FTC or State attorneys general. Authorizes the establishment of a Victims Relief Fund in the Treasury to be funded by civil penalties imposed under the Act and to be used to compensate individuals affected by violations resulting in civil penalties. Appropriates $100 million for FTC enforcement. Gives the FTC authority to issue permanent injunctions or impose equitable remedies, including restitution, recission and disgorgement. Requires the FTC to establish a program in which the FTC must approve voluntary consensus standards or certification programs that meet certain conditions, and that CEs may use to comply with one or more provisions of the Act. Compliance with the standards will be deemed compliance with the Act.	HIPAA enforceable by HHS or, for criminal violations, the Department of Justice.	
Private Right of Action	No	No	

Preemption and Relationship to Other Federal Laws	No State or political subdivision of a State may adopt or continue in effect any law or standard related to the data privacy or data security and associated activities of CEs except for state laws that directly establish requirements to notify consumers in the event of a data breach. The Act may not be construed to modify, limit, or supersede COPPA, Gramm-Leach-Bliley, HIPAA or HITECH. To the extent that the data collection, processing, or transfer activities of a CE are subject to any of these laws, those activities are not subject to the requirements of this Act.	HIPAA preempts state laws except more stringent state privacy laws.	
Effective Date	18 months after enactment		

Diane Sacks LLC

November 6, 2020

Privacy and Security Round Up

California Privacy Ballot Initiative Passes Only Weeks After Third Set of Proposed Modifications to CCPA
On November 3, 2020, California voters approved the California Privacy Rights Act of 2020 (CPRA) as a ballot initiative. The CPRA amends and expands the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020. It imposes additional restrictions on handling sensitive personal information, expands opt-out rights, add the right to correct personal information and limits service providers' permitted use and combination of personal information obtained from different sources. Businesses must comply with the CPRA beginning January 1, 2023 (generally with respect to personal information collected after January 1, 2022) and enforcement begins July 1, 2023.

Only weeks before passage of the ballot initiative, on October 12, 2020, the California Department of Justice (DOJ) issued a third set of proposed modifications to the California Consumer Privacy Act ("CCPA") regulations. Among other things, the proposed changes address how businesses that interact with consumers offline can provide the notice to opt out of sales of their personal information offline and provides guidance and examples of business methods for making opting-out of the sale of personal information easy. Comments were due by October 28, 2020.

Comments: While compliance with the CCPA will form the foundation for compliance with the CPRA, the significant and ongoing changes in the privacy landscape in California will remain a challenge for businesses operating there for at least the next few years.

ONC Issues Interim Final Rule Extends Applicability Date for Information Blocking Rule
On October 29, 2020, the U.S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health IT (ONC) released an interim final rule with comment period (IFC) that extends the compliance dates for certain requirements specified in ONC's Cures Act Final Rule. Under IFC, the new applicability date for the information blocking requirements is April 5, 2021 (instead of November 2, 2020). As with the original Final Rule, this date applies only with respect to the data elements in the USCDI, and the applicability date with respect to the full scope of EHI is October 6, 2022. In addition, under the IFC, certified health IT developers will have until April 5, 2021 to meet certain Program Conditions for Certification applicable to information blocking (previously, there was an enforcement discretion until February 2, 2020 for most of these requirements). The rollout of the standardized API functionality is now required by December 31, 2022 (previously August 2, 2022). ONC states that it is issuing the IFC to provide "additional time to allow everyone in the health care ecosystem to focus on COVID-19 response." Comments are due by January 4, 2021.

Comments: ONC notes that it is providing only a 5-month extension for the information blocking requirements because of ONC's "sense of urgency in addressing information blocking," and also because the information blocking provisions do not explicitly require the purchase or update of certified health IT, and so there is "less of a concern about technology resource allocations in the near term." While some stakeholders are likely to disagree with this assessment, it is not clear what additional information or circumstances would persuade ONC to extend the date further.

OCR Announces More Settlements for Potential HIPAA Violations
On October 28, 2020, the HHS Office of Civil Rights (OCR) announced that Aetna had agreed to pay $1 million to settle potential HIPAA violations arising from several breach reports in 2017. The first involved two web services that allowed access to member protected health information (PHI) without login credentials. The second involved the unintended disclosure of the words "HIV medications" through a window envelope and the third, the display of the name and logo of a research study sent to participating members. OCR's investigation found that, among other things, Aetna failed to

implement procedures to verify the identity of those seeking access to PHI, limit PHI disclosures to the minimum necessary, and have in place appropriate safeguards to protect PHI.

On October 30, 2020, OCR announced that the City of New Haven, CT, had agreed to pay $202,400 to OCR to settle potential HIPAA violations arising from a former employee being able to access PHI through her workplace computer and login credentials eight days after being terminated. OCR found that, among other things, the City had failed to conduct an enterprise-wide risk analysis, implement termination procedures, or access controls.

On November 6, 2020, OCR announced a tenth HIPAA settlement in its "HIPAA Right of Access" initiative, this time with Riverside Psychiatric Medical Group in the amount of $25,000 for refusing to provide medical records on the basis that some of them were psychotherapy notes. OCR found that the records that were not psychotherapy notes should have been provided to the patient.

Comments: The two larger settlements illustrate the costly impact of avoidable HIPAA errors and, as in most OCR cases, came to light as a result of OCR investigations following breach reports by the entities involved.

Federal Agencies Warn Healthcare Facilities of Cybersecurity Threats

On October 28, 2020, the Cybersecurity and Infrastructure Agency (CISA), FBI and HHS issued a joint cybersecurity advisory that they had "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." The Advisory provides detailed information on potential ransomware attacks for financial gain and provides various security best practices to protect against the threat.

Comments: As the Advisory notes, these issues will be particularly challenging during the COVID-19 pandemic, and therefore, organizations "will need to balance this risk when determining their cybersecurity investments."

FCC Issues Proposed Rule on TCPA Exemptions to Implement TRACED Act

On October 1, 2020, the Federal Trade Commission (FCC) issued a **Notice of Proposed Rulemaking** (NPRM) seeking comments on implementing provisions of the TRACED Act with respect to certain exemptions under the Telephone Consumer Protection Act (TCPA). Section 8 of the TRACED Act requires the FCC to ensure that certain requirements are imposed for these TCPA exemptions, including specifying the classes of callers and call recipients and the number of permissible calls. These requirements would apply to the exemption for HIPAA calls to a residential line and the health care provider exemption for calls to a wireless number. The NPRM proposes to codify the health care provider exemption in regulation, and to require callers to allow consumers to opt out of HIPAA calls to a residential line. Comments were due by October 26, 2020.

Comments: The NPRM had a very short comment period, presumably because the TRACED Act requirements must be implemented by December 30, 2020. This is unfortunate, since the NPRM could result in the FCC imposing significant new restrictions on TCPA exemptions for health care calls at a time when health care organizations need more, rather than less, flexibility to reach consumers regarding important health care issues.

HHS Publishes Health IT Strategic Plan for 2020-2025

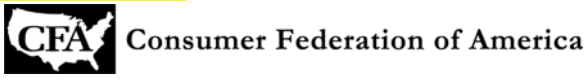
On October 30, 2020, HHS announced the publications of its final Health IT Strategic Plan for 2020-2025. The Plan outlines federal health IT goals and objectives, with a focus on individuals' access to their electronic health information.

Comment: The Plan does not appear to break new ground in terms of HHS's health IT initiatives or goals.

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.

Privacy And Digital Rights For All

A blueprint for the next Administration



Introduction

We are a coalition of leading privacy, civil rights, and consumer organizations that have come together to develop a policy framework for protecting the privacy of all people in the United States. We are particularly concerned about protecting the most vulnerable segments in our society, including Black and Brown communities, children, and low-income populations. We are advocating for federal baseline privacy legislation and action by government agencies to protect individuals from discriminatory data processing practices and to ensure their privacy rights.

The United States is facing an unprecedented privacy and data justice crisis. We live in a world of constant data collection where companies track our every movement, monitor our most intimate and personal relationships, and create detailed, granular profiles on us. Those profiles are shared widely and used to predict and influence our future behaviors, including what we buy and how we vote. Through a vast, opaque system of algorithms and other automated decision-making processes, we are sorted into categories based on data about our health, finances, location, gender, and race.

The impacts of this commercial surveillance system are particularly harmful for communities of color and low-income populations, fostering discrimination in employment, government services, healthcare, education, and many other institutions. In the absence of civil rights and anti-discrimination protections for the digital marketplace, Big Data systems can produce disparate outcomes exacerbating existing hierarchies and inequities in our society.

Children and teens require special attention from policymakers. While there are some existing government privacy protections for the youngest children, the explosive growth of the online digital marketplace has made young people of all ages vulnerable to an onslaught of aggressive marketing and data collection practices that require additional safeguards.

Without laws that limit how companies can collect, use, and share personal data, we end up with an information and power asymmetry that harms consumers and society at large. Individual, group and societal interests are diminished, and our privacy and other basic rights and freedoms are at risk.

We urgently need a new approach to privacy and data protection. The time is now.

The U.S. public strongly supports new laws that will protect privacy and digital rights. Recent polling from the Pew Research Center found that 3 out of 4 Americans believe there should be more government regulation of what companies do with their data. In another poll from Morning Consult, 79 percent of respondents agreed that Congress should craft a bill that improves their privacy rights. In the face of rising concerns over the harmful data practices of the technology industry, this Congress has made progress towards crafting effective federal privacy legislation, with bipartisan agreement on the need for a federal privacy bill.

The COVID-19 pandemic has highlighted the need for a comprehensive baseline U.S. privacy law. Technology companies, remote-learning providers, and employers are taking advantage of the pandemic to collect troves of personal data. We need presidential leadership to address these challenges.

While some solutions are legislative, we encourage the Administration to prioritize and act swiftly to put in place privacy and data justice protections: affirming privacy, surveillance, and corporate concentration issues as critical racial justice issues; ending the surveillance of Black and Brown communities; protecting the privacy of federal employees; eliminating bias and disparate impacts in government programs by requiring the federal government and companies with federal contracts to follow exemplary privacy and data justice practices; encouraging robust and meaningful agency enforcement; and supporting action in Congress to enact effective privacy laws. To that end, we urge you to adopt the following ten action items starting next year. We are available to assist in drafting any orders, memos, and policies mentioned below.

Please note: A broad group of leading privacy, consumer and civil rights organizations produced this memorandum to underscore the importance of bold action in digital rights and privacy. Because the organizations involved and the issues addressed are diverse, not every organization works on or endorses each item listed, although all firmly support the vast majority. The organizations are unanimous in their support for pro-consumer and pro-citizen action on these issues.

Action 1: Recognize Privacy and Surveillance as Racial Justice Issues, and Enact Meaningful Changes to Protect Black and Brown Communities

Recommendations for Day One

- Send a memorandum across the Administration reiterating the need for privacy protection that specifically addresses racial justice. This memo should urge the Department of Justice (DOJ) to promulgate guidance that Title VI of the Civil Rights Act of 1964 prohibits discriminatory data processing practices in determinations about federal financial assistance.

Recommendations for First 100 Days

- Require impact assessments from agencies about the use of algorithms and other automated processes in federally financed programs, including outsourced data processing, impact assessments of disparate impacts caused by these processes, and plans to eliminate those disparate impacts.

- Direct all agencies with civil rights authorities to evaluate discriminatory processing of personal data in their jurisdictions, engage in rulemaking or enforcement actions to eliminate discriminatory processing of personal data, and make legislative recommendations if additional authorities are necessary. This includes but is not limited to the Department of Justice, Department of Housing and Urban Development, Equal Employment Opportunity Commission, Consumer Financial Protection Bureau, Food and Drug Administration, Federal Trade Commission, Department of Homeland Security, Department of Health and Human Services, Department of Labor, Department of Agriculture, and Department of Education.

- Direct agencies not to adopt the use of algorithms or other predictive models as a safe harbor or defense against disparate impact claims or other claims that prohibit racial discrimination.

- Establish an Interagency Task Force on Data Privacy and Justice, with participation from the FTC, DOJ, and other relevant agencies with the goal of developing tools to identify and eliminate data practices with disparate impact.

Action 2: Establish Algorithmic Governance and Accountability to Advance Fair and Just Data Practices

Recommendations for First 100 Days

- Establish a National Algorithmic Accountability Initiative to investigate how new data-gathering techniques, digital advertising, and automated decision-making may have discriminatory or disparate impacts in areas such as housing, employment, health, education, voting rights, and lending.
- Task the Initiative with producing recommendations for legislative and regulatory principles, to be adopted in federal privacy legislation.
- Ensure an open and inclusive process for U.S. policy on AI.
- Require that any AI system adopted by an agency be supported by a valid public purpose, thoroughly vetted, and backed by accountability measures that allow a person unduly harmed by the system to obtain redress.

Recommendations for Year One

- Require law enforcement and intelligence agencies to conduct algorithmic impact assessments for their use of automated systems.
- Urge the Securities and Exchange Commission (SEC) to require public companies to disclose in their shareholder disclosures how the company processes personal data, including algorithmic processing.

Recommendations for Legislative Action

- Promote federal privacy legislation that requires algorithmic accountability (including impact assessments); incorporates the principles of transparency, accountability, and oversight; and establishes criteria for permissible automated decision-making processes.
- Promote legislation based on the Universal Guidelines for Artificial Intelligence, the first human rights framework for AI in U.S. law, and the OECD AI Principles as a baseline for AI regulation.

See more recommendations for establishing algorithmic governance here.

Action 3: Promote Privacy Protections and Encourage Enactment of a Baseline Comprehensive Federal Privacy Law

Recommendations for First 100 Days

- Appoint a White House Data Privacy and Justice czar.
- Issue an executive order to protect federal employees from inappropriate data collection, consistent with the Privacy Act of 1974.
- Issue an executive order to restrict government contracts to companies that protect privacy, consistent with the Privacy Act of 1974.
- Ensure that any trade negotiation or prospective outcome on digital trade talks must prioritize consumer protections and rights, e.g. by protecting people's privacy rights and personal data protection, and ensuring algorithmic transparency and accountability.
- Ensure that individuals' personal data coming into the U.S. from abroad, as well as data about those in the U.S. being processed abroad, receives protections that reflect highest global civil liberties and privacy standards.

Recommendations for Legislative Action

- Urge Congress to pass federal privacy legislation. This legislation should:
    - Restrict the collection, use, storage, and transfer of data to permissible purposes (rather than including 'opt in' or 'opt out' consent models).
    - Ensure civil rights protections, algorithmic accountability, and safeguards for fairness and equity online.
    - Prohibit "take it or leave it" terms.
    - Guarantee a private right of action so individuals can enforce their rights and corporations can be held accountable.
    - Establish a federal floor for privacy protection, not a ceiling.
- Encourage Congressional ratification of the Council of Europe Convention 108+. This convention supports innovation and user privacy rights and is the only binding international treaty on data flows and personal data protection.

Action 4: Establish a Data Protection Agency

Many democratic nations have a dedicated data protection agency with independent authority and enforcement capabilities. While the FTC helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority on privacy. Furthermore, the agency has failed to enforce the orders it has obtained. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations.

Recommendations for First 100 Days

- Establish a White House Task Force on how to bring data, privacy, and digital rights work under one roof leading up to, during, and after the establishment of a data protection agency.

Recommendations for Legislative Action

Urge Congress to establish a data protection agency, with the adequate resources, rulemaking authority and enforcement powers to:

- Promulgate rules to protect the privacy and security of individuals' personal information;
- Ensure fair contract terms in the market, including by prohibiting "pay-for-privacy provisions" and "take-it-or leave it" terms of service;
- Examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations;
- Require meaningful changes in business practices and issue penalties in response to violations; and
- Cooperate with other agencies on overlapping issues such as antitrust, consumer protection, and civil rights.

See more on the need for and uses of a data protection agency here.

Action 5: Ensure Robust Enforcement from the FTC and FCC

Recommendations for Year One

Encourage the FTC and the Federal Communications Commission (FCC) to:

- Make clear that they will take appropriate action under their existing authority to enforce compliance with individuals' privacy rights, recognizing that violations of those rights constitute consumer harm.
- Apply meaningful penalties that have a real impact on noncompliant companies' bottom lines.
- Require meaningful changes in business practices in response to violations.
- Commission 6(b) studies to identify discriminatory processing of personal data in products and services aimed at children, in the ad tech and ed tech industries, in communications, in direct-to-consumer DNA testing, and in other areas over which they have jurisdiction.
- Use their authority to the fullest extent possible to promulgate rules that define unfair and deceptive trade practices, regulate the data practices of companies such as smart grid providers and auto manufacturers, and can result in penalties for first-time violations, if appropriate.

See more on recommendations for stronger enforcement here.

Action 6: Bring Consumer, Privacy, and Civil Rights Experts into Key Government Positions

Recommendations for First 100 Days

Ensure that the people who are selected for positions that involve the technology industry, data, privacy, and digital rights (including but not limited to the DOJ, FTC, FCC, and aforementioned data protection agency) exemplify the following characteristics:

- Be representative of the country, with diversity in race, gender, orientation, and disability;
- Have demonstrated a commitment to civil rights, privacy, and racial justice both online and off;
- Have demonstrated a fluency in digital rights, data, and technology issues, as well as the problems of disparate impact and algorithmic discrimination; and
- Do not have significant conflicts of interest. The Office of Government Ethics should be given the authority to conduct a screening process and recommend against proposed appointees for senior level positions if their employment backgrounds and/or current private sector activities would give rise to potential conflicts of interest requiring recusal.

Action 7: Limit Government Surveillance and Access to Personal Data

Recommendations for Day One

- Ban or place a moratorium on facial recognition and other biometric surveillance by federal authorities.
- Improve oversight and reporting requirements for location data surveillance.
- Immediately stop disproportionate federal government collection, use, storage, and surveillance of personally identifiable information.

Recommendations for Legislative Action

- Promote federal privacy legislation (discussed earlier in this memo) that includes clear limits on government access to personal data, including requirements for:
    - A warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order to obtain personal data;
    - Clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
    - Providing prior notice to the individual concerned, with reasonable exceptions, and the ability of individuals to contest the data request.
- Reform U.S. surveillance laws in response to the European Court of Justice's decision invalidating the EU-U.S. Privacy Shield agreement, including ending bulk collection conducted under EO 12333 and expanding the role of the FISA court in overseeing surveillance under EO 12333 and Section 702.

See more recommended principles for protecting citizens' data from inappropriate law enforcement access here.

Action 8: Protect Children and Teens from Corporate Surveillance and Exploitative Marketing Practices

Recommendations for First 100 Days

- Urge the FTC to begin 6(b) studies on ad tech and ed tech companies' data practices and their impacts on children and teens before undertaking any rulemaking under the Children's Online Privacy Protection Act (COPPA).
- Protect students through an executive order that requires the Department of Education (DoE) to:
    - Prohibit the selling or licensing of student data;
    - Issue recommendations on transparency and governance of algorithms used in education; and
    - Minimize data collection on students, ensure parental consent is affirmatively obtained before disclosing student data, and issue rules enabling parents to access and also govern data on their child.

Recommendations for Legislative Action

- Ensure children and teen privacy is legislatively protected as part of a comprehensive baseline federal privacy bill that:
    - Establishes the special status of children and teens as vulnerable online users; provides strong limits on collection, use, and disclosure of data, and narrowly defines permissible uses;
    - Requires employing privacy policies specific to children's data on all sites and platforms used by children; and
    - Prohibits targeted marketing to children and teens under the age of 18 and profiling them for commercial purposes.
- Strengthen COPPA by raising the covered age to 17 years and under, banning behavioral and targeted ads, banning the use of student data for advertising, and requiring manufacturers and operators of connected devices and software to prominently display a privacy dashboard detailing how information on children and teens is collected, transmitted, retained, used, and protected.

See more recommended principles for protection of children and teens here.

Action 9: Ensure Antitrust Authorities Take Privacy, Digital Rights, and Civil Rights into Account in Merger Review Process

Recommendations for First 100 Days

- In the memorandum about digital rights, privacy, and racial justice that is called for in Action 1, affirm that corporate concentration is also a racial justice issue that should be prioritized, along with privacy issues, in antitrust enforcement.
- Develop an integrated policy and enforcement approach within and among relevant agencies to address competition, privacy, digital rights, and civil rights issues.
- Direct antitrust enforcers to consider privacy and data protection in merger reviews.

Recommendations for Legislative Action

- Encourage Congress to address digital rights and antitrust reforms to prevent corporate concentration among Big Tech companies.

Action 10: Protect Americans' Health Data

Recommendations for First 100 Days

- The executive branch, independent agencies and Congress should review the impact of federal policies regarding digital technologies in health, including current data collection, the use of analytics, data storage, and data transfer practices at the consumer and provider level. For example:
    - HHS should assess how well the Health Insurance Privacy Protection Act (HIPAA) protects the confidentiality and privacy of individuals' health data and identify gaps in protection.
    - HHS should also assess the privacy impact of its policies for sharing patient electronic health records.
    - The FDA should assess its policies for digital medical and non-medical devices.
    - The U.S. Centers for Medicare & Medicaid Services should assess its policies concerning distance healthcare, HIPAA and other existing law pertaining to patient data, current data collection, use (including analytics), storage, and transfer practices at the consumer and provider level.
    - Recommendations on revisions of HIPAA, as well as in federal privacy legislation to maximize protections for patients/health consumers amidst rapidly developing technologies.
- Develop proposals at all levels of government to limit the use of personal data to make health-related inferences and to maximize privacy protections for patients and health consumers.
- Provide guidance and recommendations for federal, state, and local agencies on appropriate use of individuals' personal data to combat the COVID-19 pandemic.
- Protect workers' health-related data from inappropriate access and use as the "workplace" expands into the home and to employees' personal lives.

Attachment #6

Privacy & Data Security Law News

California Harmonizes CCPA, HIPAA But Providers Still Face Obligations

By Brandon Reilly

Oct. 27, 2020, 4:00 AM

California lawmakers have helpfully clarified and harmonized the CCPA's applicability to patient information. However, in doing so, they introduced new obligations that may fly under the radar for health-care companies that have not closely followed the CCPA due to its health-related exemptions. Brandon Reilly, partner with Manatt, Phelps & Phillips LLP, offers tips to mitigate compliance risks.

In a little-noticed amendment, California legislators responded to the call of health-care companies and privacy advocates and recently expanded the California Consumer Privacy Act's exemptions of patient information to include research data and more information handled by business associates, and harmonized the law's de-identification exemption with the federal Health Insurance Portability and Accountability Act.

However, in doing so, AB 713 also created a novel restriction on re-identification and introduced public disclosure and contract obligations that may be surprising to health-care entities unaccustomed to CCPA compliance.

It is a common misconception that health-care companies enjoy a blanket exemption from the CCPA, California's groundbreaking consumer privacy law. In fact, the CCPA exempts no health companies at the entity level and instead employs a clutter of exemptions targeting health-related data sets.

While the effect may sometimes be similar to that of a blanket exemption, peripheral data sets often remain subject to CCPA regulation, which can include marketing lists, web tracking data, and employee information. By adding obligations that linger even after data has been deidentified, AB 713 only adds to the often subtle compliance risks that the CCPA poses to the health industry.

How Does AB 713 Expand CCPA's Exemptions of Patient Information?

The California Legislature answered calls from an alliance of providers, medical researchers and privacy groups by expanding and simplifying the CCPA's current exemptions relating to patient information. Before AB 713, the CCPA utilized the following patchwork of exemptions relevant to patient information:

Attachment #6

1. Information collected by a covered entity or business associate and regulated as protected health information (PHI) by HIPAA or its California corollary, the California Medical Information Act.
2. Other information collected by a covered entity—but not a business associate—and "maintained in the same manner" as PHI.
3. Information collected as part of a clinical trial subject to the Common Rule.
4. Information that is de-identified under the CCPA's novel de-identification standard which does not incorporate HIPAA's own long-standing de-identification rule.

In response to requests to better align the CCPA with existing health privacy regulations, AB 713 enhances these exemptions in three ways. First, the narrow exemption for clinical research is broadened to cover any information that is collected, used or disclosed in any medical research, if conducted in accordance with applicable laws and ethics.

Second, information that a business associate "maintains in the same manner" as PHI is now exempted, expanding the important exemption previously available only to covered entities. This fix cures the original CCPA's puzzling protection of such information maintained by a covered entity but not its business associate.

Third, personal information that is de-identified pursuant to the HIPAA Privacy Rule's two available de-identification methods—expert determination and safe harbor—is now exempt, fixing a theoretical gap between the two laws' de-identification standards. Information that is subsequently re-identified is no longer exempt and re-identification is now largely prohibited.

The Surprise of New Obligations

The cleaned-up de-identification exemption comes with strings attached. Whereas HIPAA is largely silent on the use or disclosure of de-identified PHI, this information is subject to new constraints under AB 713. Health-care companies are well advised to revisit their CCPA compliance efforts to ensure they are meeting these new obligations.

In what appears to be a first-of-its-kind prohibition, under AB 713, California law now explicitly bans any re-identification of de-identified patient information (DPI) unless certain exceptions apply. These exceptions include where data is re-identified for purposes of HIPAA-regulated health care or payment operations or pursuant to regulated public health activities or research or as otherwise permitted by law.

AB 713 now also requires public disclosure of any sale or sharing of DPI and new contractual restrictions covering the sale or license of such information.

Specifically:

1. Businesses must publicly disclose any selling or sharing of DPI and that the information was de-identified pursuant to HIPAA standards.
2. Contracts for the sale or license of DPI must:
    1. State that the sold or licensed data includes DPI.
    2. Prohibit any re-identification or attempted re-identification.

Attachment #6

3. Prohibit further disclosure of DPI to third parties unless the third party is contractually bound by the same or stricter restrictions, unless otherwise required by law.

These new requirements mean that a surprise may be in store for health-care companies that have assumed that their data sets are largely unregulated by the CCPA but regularly share, sell or license their DPI.

Impact of the California Ballot Initiative

A new privacy law, the California Privacy Rights Act (CPRA), is being presented to California voters even as the CCPA remains in its infancy. If enacted, the CPRA would replace and enhance the CCPA. How would AB 713 be impacted?

Fortunately for health-care businesses, AB 713's drafters protected most of its provisions in brand-new sections of the state civil code that will remain even if the CPRA replaces the CCPA. As a result, programmatic changes implemented by companies in response to AB 713 can largely remain.

The requirement to disclose DPI sales or sharing, however, appears in an existing CCPA provision and would appear to be nullified if the CPRA passes.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Write for Us: Author Guidelines

Author Information

Brandon Reilly is a partner with Manatt, Phelps & Phillips LLP in its privacy and data security practice where he counsels clients on a wide array of consumer protection and privacy matters, including data privacy and security compliance and procedure and data breach response.

Cybersecurity: One in three attacks are coronavirus-related

NCSC annual review says agency is putting more effort into protecting healthcare.

By Danny Palmer
November 3, 2020 3:25AM PST
ZDNet

The UK's National Cyber Security Centre (NCSC) is 'stepping up support' for the National Health Service to help protect UK hospitals and other healthcare organisations against cyberattacks.

The NCSC's Annual Review 2020 reveals that the cyber arm of GCHQ has handled more 200 cyber incidents related to coronavirus during the course of this year – almost a third of the total number of incidents it was called in to help with over that period.

And due to the urgency of securing healthcare during the coronavirus pandemic, the NCSC has been helping the NHS to secure itself against cyberattacks.

That includes performing threat hunting on 1.4 million NHS endpoints in an effort to detect potentially suspicious activity and scanning over one million NHS IP addresses to detect cybersecurity weaknesses.

"The second half of the year for us, as it has for everyone else, has been dominated by the response to COVID," said Lindy Cameron, CEO of the NCSC.

"What we've done as an organisation is really pivot towards the health sector to try and give them the best support we can in thinking about their cyber defence to let them focus on responding to the pandemic," she added.

The NCSC also helped roll out Active Cyber Defence services, including Web Check, Mail Check and protective DNS, to 235 front-line health bodies across the UK, including NHS Trusts to help protect them against phishing attacks and other threats.

"We've taken our active cyber-defence portfolio and pivoted it towards the health sector with 230 health bodies using our active cyber defence. That's all part of the support we've given to NHS Digital to help them help the health sector," Dr Ian Levy, NCSC technical director, told ZDNet.

"We're stepping up our support quite significantly," he continued, adding: "Obviously it's still for individual trusts to protect themselves along with NHS Digital and ourselves, but we're really trying to take them the knowledge about the threat and actioning support in the sector at large".

More than 160 instances of high-risk vulnerabilities have been shared with NHS Trusts during the course of this year while the NCSC has also had to to deal with over 200 incidents related to the UK's coronavirus response – including Russian cyber espionage targeting coronavirus vaccine development.

The 200 coronavirus-related incidents make up a significant chunk of the total number of 723 cyberattacks involving almost 1,200 victims that the NCSC has helped deal with during the course of the past year, a figure up from 658 in the previous year – and the highest number of incidents since the NCSC was set up. It's also a number that's likely to continue rising as cyber criminals get more ambitious.

The review also notes that the NCSC has dealt with three times more ransomware attacks than it did last year as attacks become more targeted and more aggressive.

"The expertise of the NCSC, as part of GCHQ, has been invaluable in keeping the country safe: enabling us to defend our democracy, counter high levels of malicious state and criminal activity, and protect against those who have tried to exploit the pandemic," said Jeremy Fleming, director of GCHQ.

"The years ahead are likely to be just as challenging, but I am confident that in the NCSC we have developed the capabilities, relationships and approaches to keep the UK at the forefront of global cybersecurity," he added.

Palantir to Help U.S. Track Covid-19 Vaccines

Data-mining company is developing a tool that health authorities plan to use to monitor the manufacture of coronavirus vaccines and determine where they should go

Palantir's technology is already being used by Health and Human Services to track hospitals' Covid-19 data.

By Peter Loftus and Rolfe Winkler
October 22, 2020 7:47 AM EDT
The Wall Street Journal

Data-mining company Palantir Technologies Inc. is helping the federal government set up a system that will track the manufacture, distribution and administration of Covid-19 vaccines, state and local health officials briefed on the effort said.

Palantir has been developing software that federal health officials would use to manage the various vaccine data and identify any issues that could prevent Americans from getting the shots, according to the health officials and materials reviewed by The Wall Street Journal.

The system, Tiberius, marks an attempt to use cutting-edge data science to help the federal government manage the work of protecting Americans against Covid-19.

It would build on work that Palantir, which was credited with helping the U.S. military track down Osama bin Laden and developed the software that immigration authorities have used to find illegal immigrants, has been doing for federal health officials tracking coronavirus hospitalizations.

State and local health officials who are setting up programs for vaccinating residents said the Tiberius system could further their efforts by, for example, identifying high-priority populations and then allocating shots to health-care workers, the elderly and others at highest risk of infection.

Yet Palantir's involvement could draw fire from some Democrats and privacy advocates who have previously expressed concerns about the company gaining access to sensitive personal health information.

Another Palantir data collection and analysis tool, called HHS Protect, which is similar in scope to Tiberius and used by the U.S. Health and Human Services Department to track hospitals' Covid-19 data, has been criticized by some for its complexity.

The state and local health officials said they were told during a recent briefing by federal counterparts that Palantir was involved in the effort. A spokeswoman for the Department of Health and Human Services said Tiberius uses Palantir technology, with Palantir serving as a subcontractor.

The Tiberius system won't have access to personal health information, said Claire Hannan, executive director of the Association of Immunization Managers, whose members manage state and local government vaccination programs. An HHS spokeswoman said no personally identifiable information will be brought into Tiberius.

Development of the vaccine data system comes as several leading candidates are in the final stage of testing and nearing results about effectiveness and safety that could prompt the U.S. Food and Drug Administration to authorize wide use.

In preparation, federal health officials have asked state counterparts to begin planning for the distribution of any authorized vaccine doses as early as November, in what may become one of the biggest U.S. vaccination campaigns in decades and a key to allowing schools, businesses and other establishments to fully reopen.

State officials have drafted plans and were due to submit them to the Centers for Disease Control and Prevention by Oct. 16.

Tiberius uses the same software as HHS Protect, according to an HHS spokeswoman, which is Palantir's Foundry tool. Foundry, which collects and analyzes data, is also used by the United Nations World Food Program to direct food where it is needed, similar to how it will be used to direct vaccines for Tiberius.

The Tiberius platform would take data from federal agencies, state and local governments, and drugmakers, distributors and others involved with Covid-19 vaccines, according to documents prepared by Palantir describing the system that the Journal reviewed.

The system would allow health authorities "to integrate a wide range of demographic, employment and public health data sets to identify the location of priority populations" and to "support allocation decision making," the documents said.

The information is aimed at giving federal officials a real-time view of data about vaccines, from their testing to inventory levels and finally administration to people, the materials said.

Health officials can use analyses and maps created by the data system to plan distribution and make allocation decisions about vaccine doses, and to track delivery of vaccines to hospitals, clinics and other places giving the shots, according to the documents.

The materials include an example of a map of Alabama showing Covid-19 case trends by county. A second map overlays a vaccine-allocation scenario to see how it compares with case trends in the state.

Once vaccine doses become available, the Tiberius system is designed to allow officials "to proactively identify distribution bottlenecks, inventory constraints, and gaps in administration across key populations," the documents said.

Tiberius could be a helpful tool for determining how many people work in health-care or nursing homes in Philadelphia and allocating initial doses to the high-priority groups, said Philadelphia Department of Health spokesman James Garrow.

Utah's health department aims to use Tiberius to help plan how much vaccine to send to hospitals, clinics and doctors' offices to target specific critical populations, and see how its vaccination campaign compares with those in other states, said Jon Reid, health informatics manager with the department.

North Carolina's and Wyoming's plans also call for using Tiberius to help allocate doses.

Tiberius takes its name from the middle name of fictional "Star Trek" character James T. Kirk, an HHS spokeswoman said. The multiagency initiative to find a Covid-19 vaccine is dubbed "Operation Warp Speed," also a nod to "Star Trek."

Palantir, based in Denver, was co-founded by billionaire tech investor Peter Thiel, who serves as chairman. The company went public in September and netted a $21 billion valuation on the first day of trading.

Palantir typically provides custom software to clients to help them manage their own data, rather than taking ownership of the data itself.

The firm has long done work for the Defense Department and has worked for the U.S. Department of Health and Human Services and the agencies it oversees, such as the Centers for Disease Control and Prevention and the FDA.

Palantir has a contract with the Immigration and Customs Enforcement agency, which has used Palantir software to find undocumented immigrants in the U.S., its chief executive said in an interview last year.

Palantir's federal health-related work includes two contracts worth a total of nearly $25 million to set up the system known as HHS Protect to track hospital data such as Covid-19 patients by age group, available beds, and protective gear on hand, according to an online federal database of government spending. The Tiberius system is "leveraging the same technologies" as HHS Protect, according to the documents.

Some health authorities and Democrats have criticized HHS Protect and a related data-collection tool, because they replaced a long-used CDC tool they knew well and because the tools haven't always been up-to-date or provided useful analysis. The critics said the Trump administration could use control of the data to diminish the extent of reported Covid-19 cases in the U.S. Supporters of HHS Protect say it is more modern and easier to update to handle new types of data compared with the old CDC tool.

In July, Sen. Elizabeth Warren and other Democratic lawmakers sent a letter to Secretary of Health and Human Services Alex Azar raising concerns that Palantir hadn't disclosed what it planned to do with any personal health information collected through HHS Protect and whether any privacy safeguards were in place. The lawmakers also asked HHS for copies of all active contracts with Palantir.

HHS hasn't answered that request, according to a person familiar with it.

Supporting Secure Data Sharing, Patient Privacy During COVID-19

Regenstrief Institute is partnering with NIH and other organizations to promote secure data sharing and enhance research related to COVID-19.

By Jessica Kent
November 17, 2020
Health IT Analytics

When COVID-19 began spreading across the US, the healthcare industry quickly moved to improve its secure data sharing practices in order to accelerate research efforts and treatment development.

Because the crisis is occurring at such a large scale, leaders had to come up with a way to safely share data related to the virus among different organizations.

"When the pandemic hit, it became obvious that we should have a large COVID-19 database that people could use for research," Umberto Tachinardi, MD, MSc, chief information officer for the Regenstrief Institute and director of informatics for Regenstrief and Indiana Clinical and Translational Sciences Institute (CTSI), told *HealthITAnalytics*.

This idea led to the creation of the National COVID Cohort Collaborative (N3C), a national effort to securely collect data to help scientists understand and develop treatments for COVID-19. NIH launched the N3C as a centralized analytics platform to store and study large amounts of EHR data from people tested for the virus.

The N3C is a partnership among the National Center for Data to Health (CD2H) and National Center for Advancing Translational Sciences (NCATS)-supported Clinical and Translational Science Awards (CTSA) Program hubs, with stewardship by NCATS.

Since its launch, the initiative has expanded to include data from a range of institutions, Tachinardi noted.

"Because of its success, other healthcare organizations have started to send data to the N3C enclave, not only CTSA hubs. We're talking about close to 100 healthcare organizations that are sending data to this platform, and it's all de-identified by design," said Tachinardi.

To further preserve data security and patient privacy for the initiative, Regenstrief Institute recently announced that it will serve as the project's Honest Data Broker, employing processes and technologies to ensure N3C data are shared in compliance with HIPAA standards.

These practices will help investigators overcome the challenges of securely collecting patient-level data, which is typically fragmented and difficult to use in large-scale research.

“EHR data comes labeled with identifiers – the patient’s name, date-of-birth, insurance numbers, and zip codes. One of the things that the sites do before they send the data to the enclave is remove most of the identifiers, and they will only send a little bit of a pseudo-identifier, or close-to identifiers, authorized by HIPAA. We call that the limited data set,” Tachinardi explained.

“However, once we get rid of all those identifiers, the problem is that we cannot add more data to a patient. So, if data was sent by a laboratory and another set of data was sent by a hospital that is separated from that laboratory, we’d need some identifiers in order to link these datasets together.”

To address this issue, N3C sought to develop a solution that would enable researchers to continue to keep the identification while simultaneously allowing for patient matching – even without knowing who the patient is.

That solution, called the privacy-preserving record linkage (PPRL), eliminates the need to expose identifiers and will help Regenstrief leaders ensure N3C data is shared securely, safely, and privately.

“We’re using a technology based on cryptographic methods. Once the site strips the identifiers out of the data, the software will use pieces of all those identifiers to create a hashed token. To make sure that it's even more difficult to re-identify patients, once the hash is created, we do another scrambling of the characters that define the token. So, it's kind of a double-encryption,” Tachinardi said.

“We’re now setting up an infrastructure to start supporting sites that are sending the de-identified data to the enclave. Once they join this process, those tokens will be stored at Regenstrief. We will not store any identifier, but we will keep the tokens so we can provide the means for linking the data itself without ever exposing the identifier.”

PPRL will also help researchers associated new pieces of data with an individual without revealing the person’s identity, Tachinardi said.

“For instance, we can associate an individual with images, genomic data, social determinants, future information. When people start getting vaccinations, we can continue to track what's going on with them. This is going to be very exciting,” he said.

The N3C initiative will provide researchers and providers with critical information related to the virus and its impact on different patient populations.

“Right now, we don't know the long-term effects of COVID-19, and because this is a database of COVID-positive patients, we’ll have information that can help us learn more about the virus and its side effects,” Tachinardi said.

“The larger the cohort, the faster we'll get answers and the higher the possibility that we’ll find something new.”

Going forward, Tachinardi believes that innovations that were accelerated due to the COVID-19 pandemic will continue to serve the healthcare industry even after the crisis has passed.

“The concept of data sharing and data integration is not new, but developing an infrastructure like this in a matter of months is unprecedented,” Tachinardi concluded.

“There are a number of accomplishments that we are seeing here that can be repeated, and now we know better. So, in the event of another pandemic, we can achieve these things faster and cheaper. We can also apply these techniques to other conditions, like diabetes, cardiovascular disease, and obesity. The principles of N3C will definitely be a game changer in healthcare research.