



HIPAA and Beyond – Transforming Health Privacy Landscape

The Past, Present, and Future of Health Privacy Policy

Erin Geygan

Senior Privacy Counsel

J&J MedTech, North America

April 19, 2023

Shaping health and well-being since **1886**



We are a “keep
you healthy
your whole life”
company.

Johnson & Johnson

Johnson & Johnson

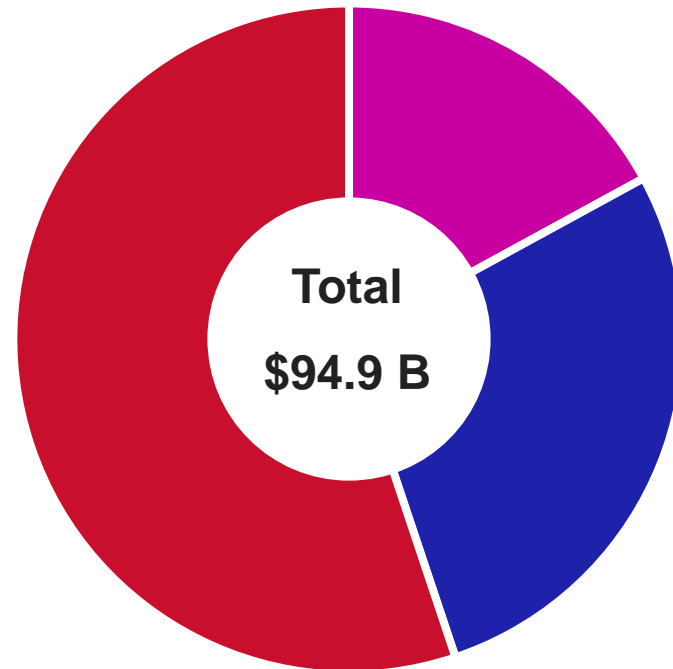
Our three business segments*

Major segments

 **Pharmaceutical**

 **MedTech**

 **Consumer Health**



**2022 Annual Report*

Johnson & Johnson

152,700 employees worldwide

\$14.6B for R&D

Johnson & Johnson

Lead in Accountability & Innovation

Our Data Privacy and Security Program

US Laws & Regulations

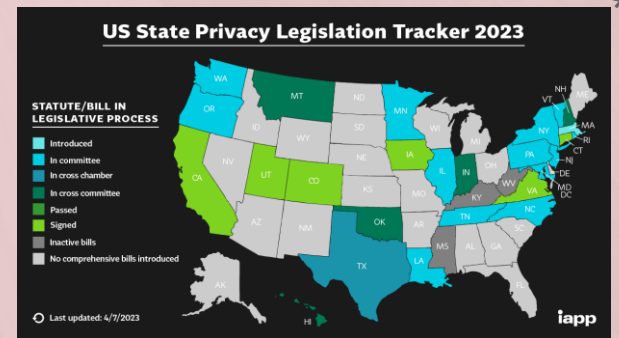
Our Data Privacy and Security Program

Federal

- HIPAA
- FTC Act
- FTC Health Breach Notification Rule
- Privacy Act of 1974
- FDA Quality Systems Regulation
- FD&C Act (including 2023 Consolidated Appropriations Act)
- COPPA
- CAN-SPAM
- Telephone Consumer Protection Act
- FCC marketing rules
- Electronic Communications Privacy Act / Wiretap Act
- Video Privacy Protection Act
- Computer Fraud and Abuse Act
- Defend Trade Secrets Act
- Sarbanes Oxley
- SEC Disclosure Rules

State

- Consumer Privacy Omnibus laws
- Data breach notification laws
- Health information privacy laws
- Biometric laws
- Wiretap laws
- Mini-FTC and TCPA Acts



* https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map.png

Global Operation

Our Data Privacy and Security Program



EU Charter of Fundamental Rights

GDPR / EU member state laws

ePrivacy Directive

NIS Directive

Cybersecurity Resilience Act

UK GDPR

FADP (Switzerland)

LGPD (Brazil)

PIPEDA & provincial laws (Canada)

PIPL, CSL, DSL (China)

IT Act & SPDI Rules (India)

APPI (Japan)

PIPA (South Korea)

POPIA (South Africa)

Company Principles

Our Data Privacy and Security Program



HIPAA – Current Perspective



Works Well



Acknowledges the vital role life sciences companies inhabit with respect to the care continuum with a focus on patients first and foremost



Provides pathways for responsible use and disclosure of patient data to promote innovation in health care to the benefit of patients, providers, insurers etc.



Promotes flexibility in implementation of compliant controls while providing a reliable and reasonable framework



Opportunities



Lack of preemption / harmonization with state laws on medical information privacy and other federal laws governing health information outside the scope of HIPAA



Address challenges facing data sharing for innovation such as technical constraints, IP risks, and niche / exclusive access

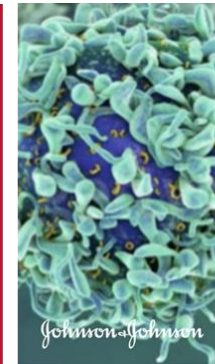


Use existing authorities to greatest extent

Future Proof Privacy

Protect & Enable

We collaborate and innovate to improve health for people everywhere.



Johnson & Johnson has been dedicated to building a healthier world for over 130 years.

We do this by helping to address some of the toughest health challenges people face. Today, those challenges include researching ways to eliminate cancer, innovating more personalized ways to perform surgery, and committing to support health equity solutions aimed at addressing racial and social justice.

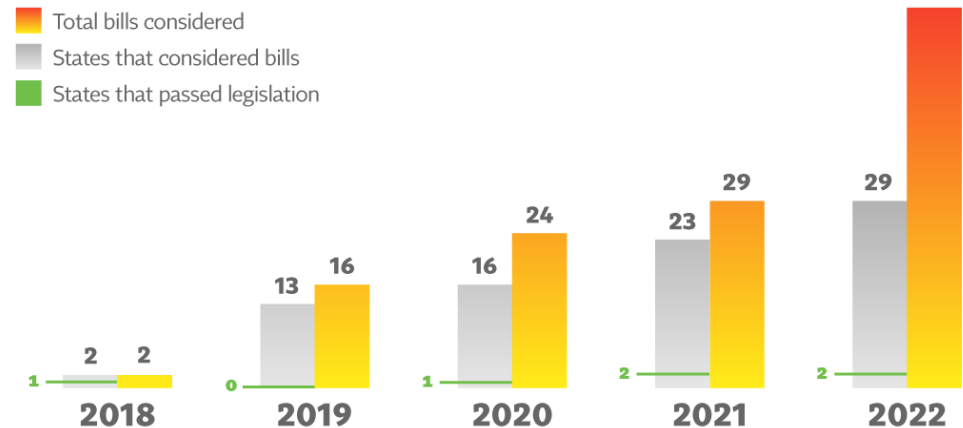
Johnson & Johnson believes that public policy on data privacy and protection should seek to provide appropriate protection and empowerment to consumers and patients while also ensuring innovation and provision of healthcare products and services are not impaired.

Harmonization & Preemption

- Additional sectoral or hyper-specialized laws further burden the compliance landscape.
- Benefits to both businesses and individuals alike, ease of understanding scope and obligations.
- Supports international operations and opportunity

The Growth of State Privacy Legislation

Comprehensive consumer privacy bills considered from 2018-2022



20 state privacy laws in progress with one omnibus law passed as of last week (IN)



62 bills proposed at federal level between 2021-2022 covering different types of data or use cases

* <https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/>

Thank you

Johnson & Johnson

Global adequacy capabilities ¹

By IAPP Director of Research and Insights Joe Jones

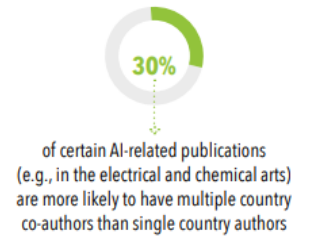
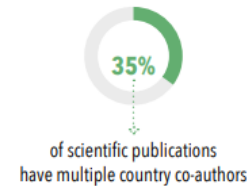


Strengthen Collaboration

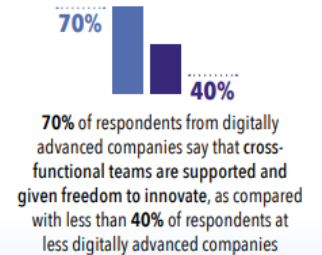
74 jurisdictions vest powers in either a data privacy regulator or government authority to designate other jurisdictions as having “adequate” data privacy standards.

DATA SNAPSHOT ON CROSS-BORDER INNOVATION ²

Research Collaboration Across Borders and Nationalities¹⁴



Inter- and Intra-Company Innovation, Including Across Borders¹⁵



WWW.GLOBALDATAALLIANCE.ORG

Abu Dhabi Global Market	Bahamas	Cabo Verde	Egypt	Gibraltar	Kazakhstan	New Zealand	Qatar Financial Centre	South Africa	Turkmenistan
Albania	Bahrain	Cayman Islands	Equatorial Guinea	Guernsey	Kenya	Niger	Republic of Korea	Switzerland	Uganda
Algeria	Bermuda	Chad	European Economic Area	Guinea	Kosovo	Nigeria	Russian Federation	Taiwan	Ukraine
Andorra	Bosnia and Herzegovina	Colombia	European Union	Indonesia	Kyrgyz Republic	North Macedonia	Sao Tome and Principe	Tajikistan	United Kingdom
Angola	Botswana	Congo	Faroe Islands	Isle of Man	Madagascar	Panama	Saint Lucia	Togo	Uruguay
Argentina	Brazil	Côte d'Ivoire	Gabon	Israel	Malaysia	People's Republic of China	Senegal	Thailand	Uzbekistan
		Dubai International		Japan	Montenegro			Trinidad and Tobago	Zambia



¹ https://iapp.org/media/pdf/resource_center/global_adequacy_capabilities.pdf

² <https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdinnovation.pdf>



THE PAST, PRESENT, AND FUTURE OF HEALTH PRIVACY POLICY

RESEARCH & DATA USE

Jessica G. Kelly

Healthcare Leadership Council
April 19, 2023

LEARNING OBJECTIVE

Review -

- Intersection of Research & HIPAA
- Privacy rule application to Research
- HIPAA Deidentification

RESEARCH PRIVACY

HIPAA, FDA & ETHICS

Privacy and Confidentiality

- Per HHS and FDA regulations (45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)), IRB must determine that, where appropriate, there are adequate provisions to protect privacy of subjects and maintain confidentiality of data in order to approve human subject research.
- Privacy and confidentiality also supported by 2 principles of Belmont Report:
 - Respect for persons—Individuals should be able to exercise their autonomy to fullest extent possible, including right to privacy and right to have private information remain confidential
 - Beneficence—Maintaining privacy and confidentiality protects participants from potential harms including psychological harms from embarrassment or distress; social harms such as loss of employment or damage to financial standing; and criminal or civil liability
- Privacy: control over extent, timing and circumstances of sharing oneself with others
- Confidentiality pertains to treatment of information that an individual has disclosed in a relationship of trust with expectation that it won't be disclosed to others without permission in ways that are inconsistent with the understanding of the original disclosure.

WHAT IS RESEARCH?

- **Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
- **Human subject** means a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.
- Institutional Review Board (IRB) - group formally designated by institution to review research involving human subjects, with authority to approve, require modification to, or disapprove all research activities covered by HHS and FDA protection of human subject regulations.
- What is not Human Subject Research –
 - Quality Improvement studies
 - Public health surveillance
 - Research and development with deidentified data

PRIVACY RULE – BEFORE RESEARCH BEGINS

- Activities preparatory to research
 - HIPAA allows certain activities “preparatory to research” (which may include allowing a researcher to review medical records to determine potential candidates for participation in a research study) to occur without an individual’s authorization, subject to the condition that the “covered entity” (i.e., health care provider such as Mayo) must obtain representations from the researcher indicating that:
 - (a) use or disclosure is sought solely to review protected health information (“PHI”) as necessary to prepare a research protocol or for similar purposes preparatory to research;
 - (b) no PHI is to be removed from the covered entity by the researcher in the course of the review; and
 - (c) the PHI for which use or access is sought is necessary for the research purposes.
- (45 CFR 164.512(i)(1)(ii))

RECRUITMENT

- Recruitment: identifying and contacting research participants
 - Identifying potential research participants: The act of identifying potential research study participants may be considered a type of “preparatory to research” activity. Guidance from the NIH indicates that a researcher who is either an employee of a covered entity or outside the covered entity is permitted to access the covered entity’s protected health information in order to identify who may qualify as a potential study subject, and that this may be done without the individual’s authorization if the covered entity obtains the representations from the researcher mentioned on the previous slide. (See <https://www.hhs.gov/hipaa/for-professionals/faq/317/can-the-preparatory-research-provision-be-used-to-recruit-individuals-to-a-research-study/index.html> and https://privacyruleandresearch.nih.gov/pdf/clin_research.pdf)

ENROLLMENT

- Contacting potential research participants: Accessing and using PHI to contact potential research subjects is a “health care operations” activity, according to NIH guidance. HIPAA allows covered entities to use and disclose PHI for health care operations activities without individuals’ authorization. However, if the researcher who will contact potential research subjects is not an employee of the covered entity, NIH guidance says the outside researcher is considered a “business associate” of the covered entity. A “business associate” is an entity or person that performs certain services on behalf of a covered entity. Covered entities are required to enter into contracts with business associates called business associate agreements, or BAAs. So, prior to allowing an outside researcher to contact potential research participants on the covered entity’s behalf, the covered entity needs to enter into a BAA with the outside researcher.

Alternatively, NIH guidance provides that a covered entity may disclose PHI to a researcher for purposes of recruiting potential subjects under a partial waiver of authorization pursuant to 45 CFR 164.512(i)(1)(i). (See https://privacyruleandresearch.nih.gov/pdf/clin_research.pdf, <https://www.hhs.gov/hipaa/for-professionals/faq/317/can-the-preparatory-research-provision-be-used-to-recruit-individuals-to-a-research-study/index.html>)

HIPAA PRIVACY RULE – RELEVANCE TO RESEARCH

- Authorization to use PHI
 - There are several exceptions which allow for use and disclosure of PHI without an individual's authorization (such as the "preparatory to research" exception and using/disclosing PHI for treatment purposes); however, in many cases, when there's no exception that fits, it's necessary to obtain an individual's authorization in order to use or disclose PHI about that individual.
 - A HIPAA authorization must contain certain elements to be effective. These elements are:
 - (i) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
 - (ii) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
 - (iii) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
 - (iv) a description of each purpose of the requested use or disclosure.
 - (v) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository. [Note that some state laws require med records authorizations to include an end date, and where more stringent than HIPAA, state law controls.]
 - (vi) signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

Additionally, the authorization must contain statements to put the individual on notice of certain things (see next slide).

HIPAA AUTHORIZATION

- Authorization to use PHI
 - Statements need to be included in an authorization to put an individual on notice of:
 - The individual's right to revoke the authorization in writing, and either: (a) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (b) a reference to the covered entity's notice of privacy practices which describes the individual's right to revoke the authorization
 - The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either: (a) the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; or (b) the consequences to the individual of a refusal to sign the authorization when the covered entity can condition research related-treatment on the individual providing authorization to use and disclose PHI for the research study
 - The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by HIPAA
- (See 45 CFR 164.508(b))

FUTURE RESEARCH

- Authorization to use PHI

- Authorizations to use PHI for Future Research

- The Office of Civil Rights or “OCR” (which is a division of the Dept. of Health and Human Services which provides guidance on, and enforces, HIPAA) released a guidance document in 2018 regarding authorizations for use of PHI in future research.
 - OCR gave the following guidance about how to adequately describe the purpose of using PHI for future research in an authorization:

“[W]ith regard to future research authorizations, the requirement to describe ‘each purpose’ means that such authorizations do not need to specify each specific future study if the particular studies to be conducted are not yet determined; rather, the authorization ‘must adequately describe such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research’” (See

<https://www.hhs.gov/sites/default/files/hipaa-future-research-authorization-guidance-06122018%20v2.pdf>)

WAIVER OF AUTHORIZATION

- Waiver of Authorization

- An IRB or a privacy board may approve a waiver or alteration of the HIPAA authorization requirement in connection with a research project. The IRB or privacy board must make the following findings in order to waive or alter the authorization requirement:
 1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
 - an adequate plan to protect the identifiers from improper use and disclosure;
 - an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
 - adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule
 2. The research could not practicably be conducted without the waiver or alteration [e.g., study involves the use of PHI pertaining to numerous individuals where contact information is unknown]; and
 3. The research could not practicably be conducted without access to and use of the PHI.

IRB WAIVER

- Waiver of Authorization

- In order for a covered entity to rely on an IRB waiver or alteration of the HIPAA authorization requirement, a covered entity must receive certain documentation from the IRB. This documentation must consist of the following:
 - The identity of the approving IRB
 - The date on which the waiver or alteration was approved
 - A statement that the IRB has determined that all the specified criteria for a waiver or an alteration (noted on previous slide) were met
 - A brief description of the PHI for which use or access has been determined by the IRB to be necessary in connection with the specific research activity
 - A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures
 - The required signature of the IRB chair or the chair's designee

(45 CFR 164.512(i))

HIPAA DEIDENTIFICATION

- De-identified Data

- HIPAA describes a process whereby PHI may be de-identified; information which has been de-identified according to HIPAA standards is no longer considered “PHI”, and therefore, not subject to HIPAA

- HIPAA recognizes 2 different methods which can be used to de-identify PHI

- (1) ‘Expert determination’ method: Under this de-identification method, “a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable” makes a determination that there is a very small risk that a recipient could identify subject(s) of information, and documents this determination.

- This method of de-identification is less commonly used and less objective than the 2nd method (removal of 18 identifiers)

- (2) Safe Harbor - Removal of 18 identifiers method: Under this method, 18 different types of identifiers of the individual (i.e., patient) or of relatives, employers, or household members of the individual, must be removed.

SAFE HARBOR

- De-identified Data

The following are the 18 types of identifiers which must be removed:

- (1) Names;
- (2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
 - (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- (3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- (4) Telephone numbers;
- (5) Fax numbers;
- (6) Electronic mail addresses;
- (7) Social security numbers;
- (8) Medical record numbers;
- (9) Health plan beneficiary numbers;
- (10) Account numbers;
- (11) Certificate/license numbers;
- (12) Vehicle identifiers and serial numbers, including license plate numbers;
- (13) Device identifiers and serial numbers;
- (14) Web Universal Resource Locators (URLs);
- (15) Internet Protocol (IP) address numbers;
- (16) Biometric identifiers, including finger and voice prints;
- (17) Full face photographic images and any comparable images; and
- (18) Any other unique identifying number, characteristic, or code (except the covered entity may assign a code or other means of record identification, provided that (i) the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (ii) The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification)

DEIDENTIFICATION METHODS

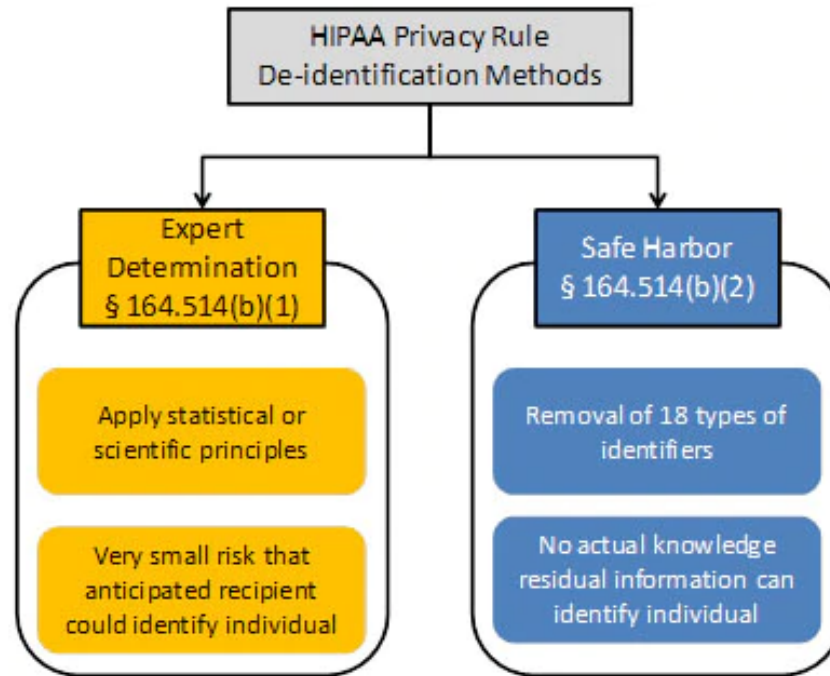


Figure 1. Two methods to achieve de-identification in accordance with the HIPAA Privacy Rule.

QUESTIONS & ANSWERS



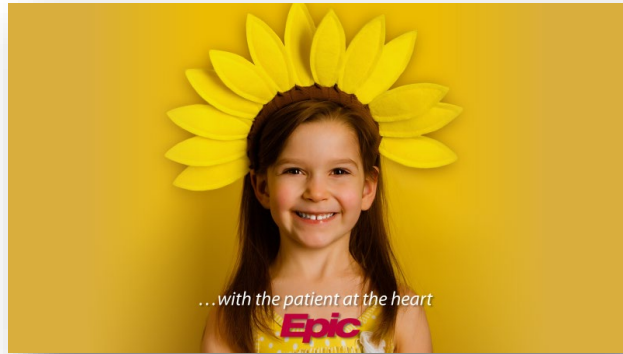
The Epic logo is rendered in a bold, italicized, red sans-serif font. It is positioned in the upper left corner of the slide. The background of the entire slide is a vibrant, abstract pattern of glowing blue and purple lines, resembling a complex network or a starry space scene.

Epic

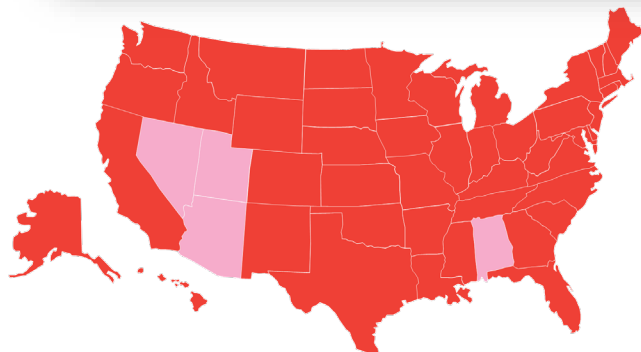
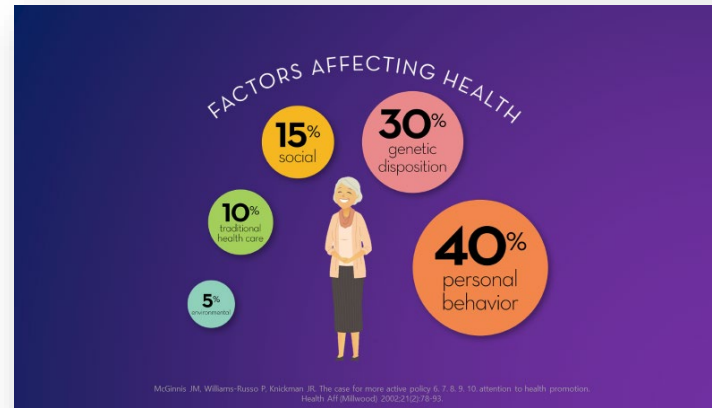
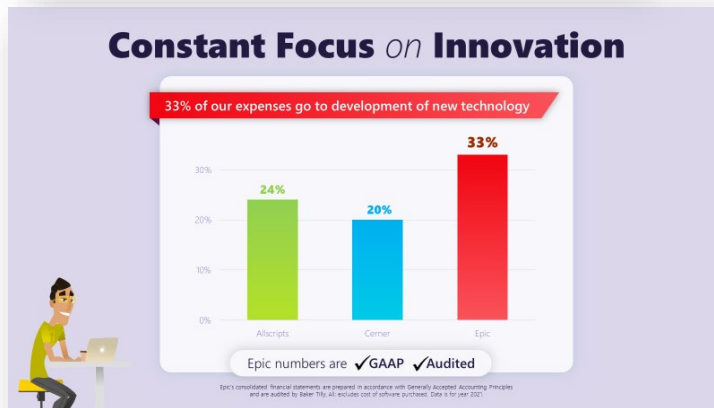
The Past, Present, and Future of Health Privacy Policy

**Amanda Reese, JD, CHPC, CPHRM
Healthcare Regulatory and Privacy Counsel**

About Epic



- Founded in 1979 in Madison, WI, by our CEO Judy Faulkner
- Grown from a founder-led start-up to the most widely-used health IT company in the US
- Almost 13,000 staff – currently in 16 countries
- All R&D done on our Verona campus



- **3,000 hospitals and 45,000 clinics**
- **400,000 EHR physicians**
- **72M patients in Cosmos**
- **The majority of retail clinics**



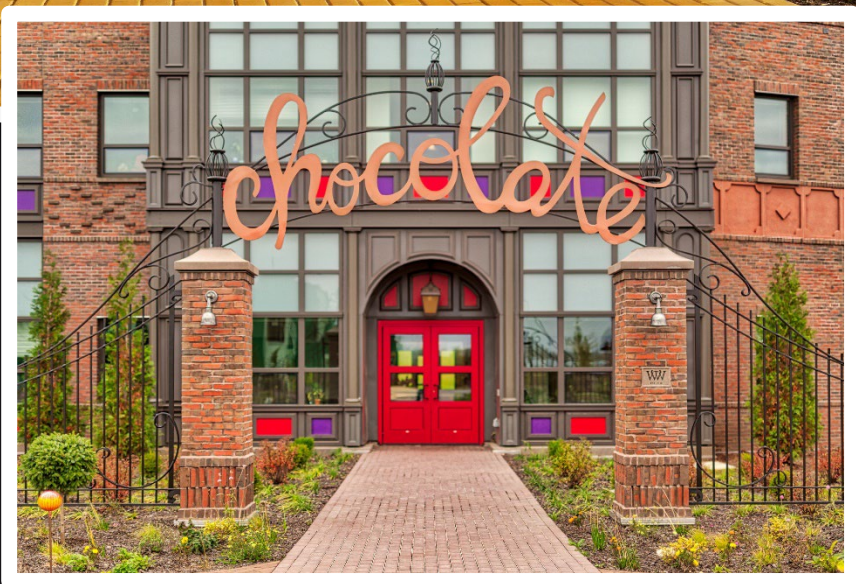
Barn

NYC Subway

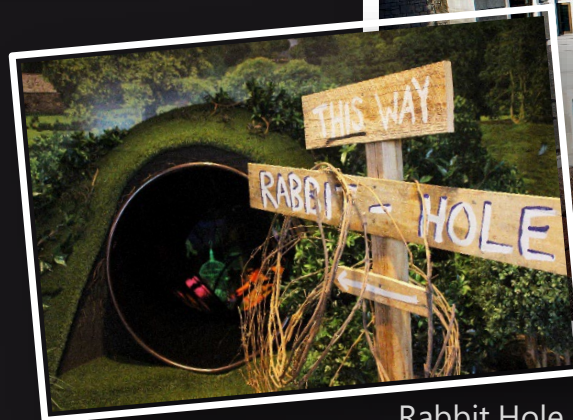
Wizard of Oz



Wizards Academy

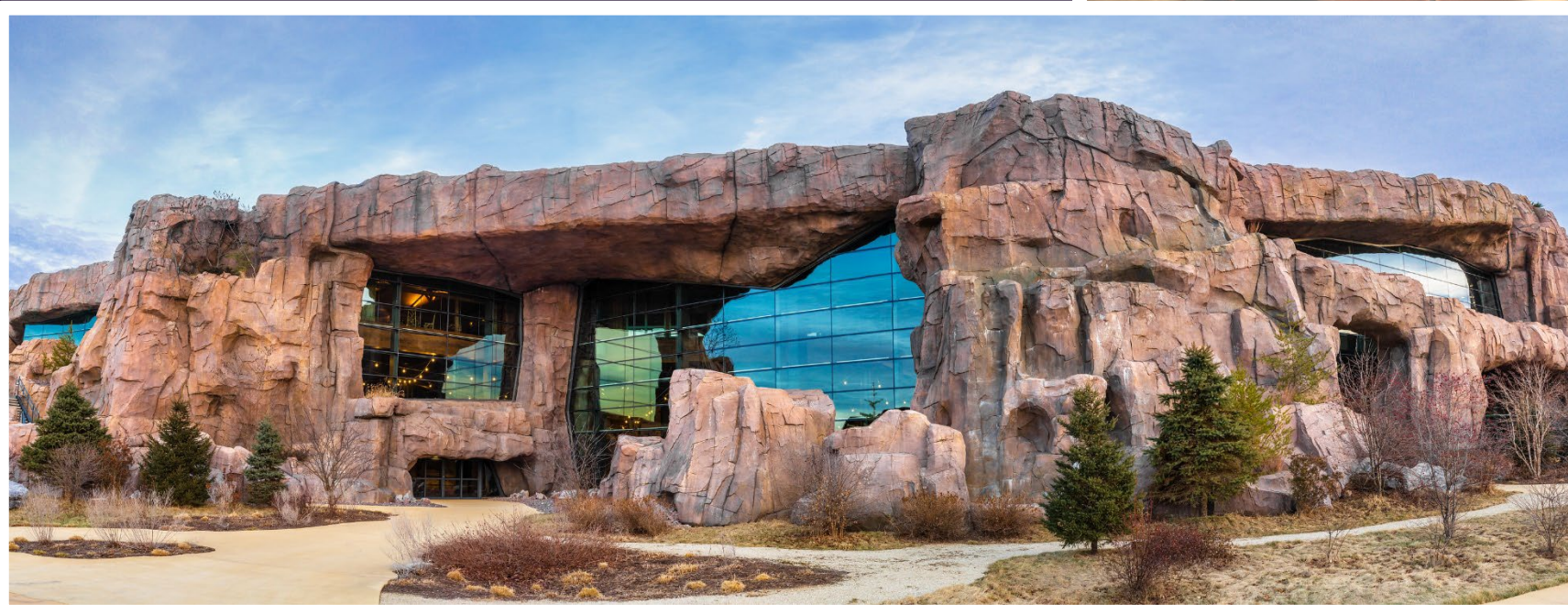


Chocolate Factory

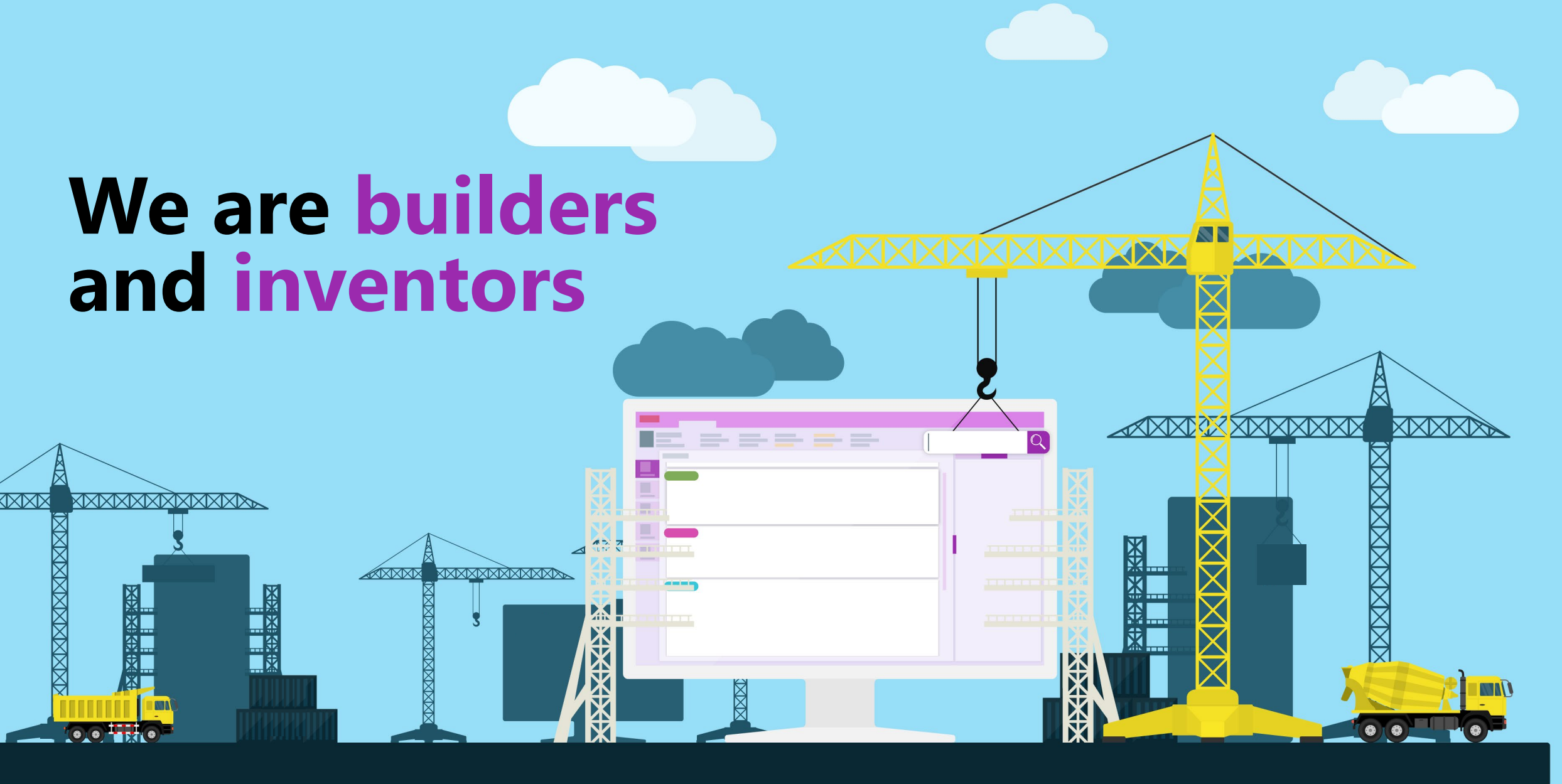


Rabbit Hole

Bring staff together monthly
Deep Space



**We are builders
and inventors**

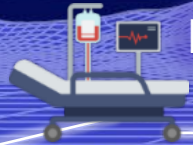


HEALTH GRID

a country-wide network with the patient at the heart



Long Term Care



Dental



Social Care



Rehab



Outpatient



Home Health



Hospice



Specialty Pharmacy



Inpatient



Urgent Care



Retail Clinics



Life Insurance



Payers



Behavioral Health



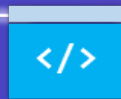
Real-Time Prescription Benefits



Specialty Diagnostics



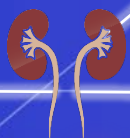
Other Apps



Home Infusion



Standalone Specialties



Employer Health



🕒 September 19, 2022

New Life Sciences Program Will Unify Clinical Research with Care Delivery



Participating providers are working with Epic to kick off the first stage of the Life Sciences program: study feasibility and clinical trial matchmaking.

- **Matching participating providers with clinical trial opportunities** suited to the makeup of their patient populations.
- **Sending participating providers purpose-built Cosmos searches** to help them validate whether a trial is right for them without the need to develop their own queries.
- **Making clinical trials accessible** to more provider groups by lowering the technical and staffing barriers to study activation.
- **Increasing clinical trial efficiency** by eliminating duplicative workflows and connecting researchers, care teams, patients, and sponsors through a single system.
- **Supporting clinicians with point-of-care insights** into when their patients might qualify for a clinical trial and applying predictive models to assist with the timing of therapy administration.

EPIC'S INTERSECTIONS WITH HIPAA

- A “business associate” of our US customers
- Abide by HIPAA's Privacy, Security, Breach Notification Rules
- Software and services support privacy
- Privacy throughout data life cycle

EPIC'S INTERSECTIONS WITH HIPAA

- Full PHI
 - *Per licenses and Business Associate Agreements*
- Limited Data Sets
 - *Per Data Use Agreements*
 - Research
 - Public Health
 - Health Care Operations
- De-identified Data
 - *Per Policies and Agreements (Depends on Data Source)*

Cosmos Data Set



1,000+
Hospitals



22,000+
Clinics



198
Live Healthcare Orgs



268K
Physicians



183 Million
Unique Patients



6.8 Billion
Encounters



1 Billion
Specialty Visits



Including

- Academic Medical Centers
- Rural Hospitals
- FQHCs

What causes autism?

How do we prevent birth defects?

How do we prevent diabetes?

What causes Alzheimer's?

Who is at risk for suicide?

Discovery

How can we cure cancer?


How can we regenerate nerves?

Who is at risk for addiction?


How can we prevent auto-immune disease?

How should we treat mental health problems?

Research Powered by


 Centers for Disease Control and Prevention
CDC 24/7: Saving Lives. Protecting People™

[A-Z Index](#)

Search 

[Advanced Search](#)

Morbidity and Mortality Weekly Report (MMWR)

CDC 

Effectiveness of COVID-19 mRNA Vaccination in Preventing COVID-19–Associated Hospitalization Among Adults with Previous SARS-CoV-2 Infection — United States, June 2021–February 2022

Weekly / April 15, 2022 / 71(15);549-555

On April 12, 2022, this report was posted online as an MMWR Early Release.

Ian D. Plumb, MBBS^{1,2,*}; Leora R. Feldstein, PhD^{1,2,*}; Eric Barkley³; Alexander B. Posner, MPH³; Howard S. Bregman, MD³; Melissa Briggs Hagen, MD^{1,2}; Jacqueline L. Gerhart, MD³ ([View author affiliations](#))

[View suggested citation](#)

Summary

What is already known about this topic?

Persons with previous SARS-CoV-2 infection have some protection against reinfection leading to hospitalization, but there is limited evidence regarding the additional benefit of vaccination among these persons.

What is added by this report?

Among persons with previous infection, COVID-19 mRNA vaccination provided protection against subsequent COVID-19–associated hospitalization. Estimated vaccine effectiveness against reinfection leading to hospitalization during the Omicron-predominant period was approximately 35% after dose 2, and 68% after a booster dose.

What are the implications for public health practice?

To prevent COVID-19–associated hospitalization, all eligible persons should stay up to date with vaccination, including those with previous SARS-CoV-2 infection.

Previous infection with SARS-CoV-2, the virus that causes COVID-19, has been estimated to confer up to 90% protection against reinfection, although this protection was lower against the Omicron variant compared with that against other SARS-CoV-2 variants (1–3). A test-negative design was used to estimate effectiveness of COVID-19 mRNA vaccines in preventing subsequent COVID-19–associated hospitalization among adults aged ≥ 18 years with a previous positive nucleic acid amplification test (NAAT) or diagnosis of COVID-19.[†] The analysis used data from Cosmos, an electronic health record (EHR)–aggregated data set (4), and compared vaccination status of 3,761 case-patients (positive NAAT result associated with hospitalization) with 7,522 matched control-patients (negative NAAT result). After previous SARS-CoV-2 infection, estimated vaccine effectiveness (VE) against COVID-19–associated hospitalization was 47.5% (95% CI = 38.8%–54.9%) after 2 vaccine doses and 57.8% (95% CI = 32.1%–73.8%) after a booster dose during the Delta-predominant period (June 20–December 18, 2021), and 34.6% (95% CI = 25.5%–42.5%) after 2 doses and 67.6% (95% CI = 61.4%–72.8%) after a booster dose during the Omicron-predominant period (December 19, 2021–February 24, 2022). Vaccination provides protection against COVID-19–associated hospitalization among adults with previous SARS-CoV-2 infection, with the highest level of protection conferred by a booster dose. All eligible persons, including those with previous SARS-CoV-2 infection, should stay up to date with vaccination to prevent COVID-19–associated hospitalization.

Tables

[Table 1](#)

[Table 2](#)

[Table 3](#)

References

Related Materials

[PDF](#)  [145K]

“Data were obtained from Cosmos (4), an EHR data set that includes more than 135 million patients and 154 health care organizations in the United States.”

without hospitalization) ≥ 30 days before the date of the NAAT associated with the subsequent hospitalization. Patients under the billing category of “observation” and patients who were admitted and discharged on the same day were excluded. Vaccination status was categorized on the day of the NAAT associated with the hospitalization as 1) unvaccinated, 2) after dose 1, 3) after dose 2, or 4) after a booster dose”; patients were excluded if they did not meet one of these definitions or if the previous positive NAAT result or COVID-19 diagnosis was after the date of the most recent vaccine dose. Vaccination information was collected during the 14 days after hospitalization or other health care visit from a patient’s health system, other health systems via clinical record exchanges, state registries, and patient-reported history.^{§§}

CHALLENGES AND OPPORTUNITIES

- Operating within the US
 - *Heavily regulated industry*
- Operating in a Global Climate
 - *Jurisdiction-specific legislation*
 - *Differing perspectives on data sharing and use*
 - *Differing goals for use of medical information*
- Balancing Data Privacy with Business Needs
- Public Views re Privacy and Healthcare