Healthcare Trust Institute

HEALTH DATA PRIVACY 101

Health data is among our most sensitive and valuable assets. Protecting it is essential to preserving trust in healthcare. This briefing explores how data privacy laws protect health information, examines the challenges facing privacy efforts, and presents actionable recommendations to strengthen privacy and safeguard public confidence

HILL BRIEFING

EXPERT SPEAKERS

surescripts

SURESCRIPTS
LAUREN JONES
CIPP/US- Sr. Privacy & Data Protection Counsel, Legal Affairs

mro

MRO
ANTHONY MURRAY
CISSP - Chief Interoperability Officer

Healthcare Trust Institute

HEALTHCARE TRUST INSTITUTE
TINA OLSON GRANDE, MHS
President and Chief Executive Officer

WEDNESDAY
APRIL 23 • 12PM ET
2045 RAYBURN BUILDING
LUNCH PROVIDED!
RSVP

healthcaretrustinstitute.com Info@hctrustinst.com 202.750.1989

Lauren Jones, CIPP/US

Sr. Privacy & Data Protection Counsel
Legal Affairs

Lauren S. Jones is Senior Privacy & Data Protection Counsel at Surescripts, providing legal, compliance, and risk management advice throughout the company. Prior to Surescripts, she served as Privacy and Data Protection Counsel at the Financial Industry Regulatory Authority and as a past project team lead for the National Institute of Standards and Technology Privacy Workforce Public Working Group. For several years, she also provided regulatory advice and legal counsel for health and human services IT interoperability and integration efforts across the District of Columbia. She is a certified information privacy professional by the International Association of Privacy Professionals.

Anthony Murray, CISSP

Chief Interoperability Officer

In his role as Chief Interoperability Officer, Murray oversees MRO's strategic initiatives related to accelerating clinical data exchange. In addition to overseeing the clinical data exchange team, Anthony also is responsible for the interoperability and systems integrations teams, to utilize advanced technologies to deliver secure, meaningful information exchange. Anthony, as a Certified Information Systems Security Professional (CISSP), and partners closely with MRO's security, privacy, compliance and innovation thought leaders, to assess all areas of the clinical data exchange and to provide value through modern, secure technologies. Anthony has over 20 years of experience in technology and security supporting the healthcare industry vertical, including release of information, clinical manufacturing and pharmaceuticals.

Tina Olson Grande, MHS

President and Chief Executive Officer

Tina Olson Grande, MHS, is President and Chief Executive Officer of the Healthcare Trust Institute (HTI), an alliance of the nation's leading healthcare organizations committed to promoting and implementing effective privacy and security protections for health information that engender trust in the healthcare system and allow for the advancement of treatments, cures and improved healthcare quality for individuals and populations. HTI members, comprised of organizations from across the U.S. healthcare economy, convene at HTI to empower innovation through trusted data privacy, security and interoperability policies - protecting what matters to drive breakthrough solutions for individuals and populations.

PRINCIPLES ON HEALTH INFORMATION PRIVACY
BOTH INSIDE AND OUTSIDE OF HIPAA

1. Robust privacy and security protections for personal health information is essential for trust in the healthcare system, which is the foundation for the delivery of quality care and patient safety.

2. All personal health information, whether falling within or outside HIPAA, should be subject to regulation to ensure that it is used in a manner consistent with an individual's reasonable expectations. Uses for other purposes should require an individual's authorization and, where feasible, privacy-enhancing technologies should be implemented.

3. Entities collecting and holding personal health information should be required to have risk-based physical, administrative and technical safeguards in place to protect that information from misuse and threats, including cyberattacks. These safeguards should evolve as technology evolves and be consistent with nationally recognized frameworks, such as the National Institute for Science and Technology (NIST) Cybersecurity Framework.

4. Protections for personal health information should be established at the national level to ensure consistency, clarity and compliance as individuals and data increasingly travel across state lines. It is also essential to avoid data masking to the detriment of patient care and safety, and to ensure that the vision of national interoperability for health data exchange can be realized, leading to better care coordination and improved health outcomes.

5. The principles of minimum necessary and data minimization should be central to collection and processing of personal health information, including through use of de-identified data or privacy-enhancing technologies where feasible. The use of de-identified data is critical to allow for important and beneficial public purposes, such as medical research and public health. To engender consumer and patient trust and public support, recipients of deidentified data should be prohibited from attempting to re-identify the data.

6. Individuals should be provided clear and simple privacy notices that explain how an entity collects and processes personal health information, as well as the individual's rights and choices with respect to their health data. These rights should generally include the right to request access and the right to request corrections.

7. The Health Insurance Portability and Accountability Act (HIPAA) framework, which has been the cornerstone for the protection of patient health information in the health care sector for almost a quarter of a century and is well-understood and trusted by patients and health care organizations alike, should remain the framework for the regulation of patient health information in the health care industry. HIPAA is tailored to health care delivery and payment, and permits the sharing of medical information for treatment, payment and healthcare operations consistent with the reasonable expectations of patients.

Updated: May 2024

8. Regulation of personal health information outside the HIPAA regulations should harmonize with the HIPAA framework, using similar concepts and definitions where appropriate, such as treating data deidentified in accordance with HIPAA as deidentified data for all purposes.

9. Privacy protections must be enforced through meaningful penalties and a mechanism for individuals to be able to report violations without fear of retaliation.

State Carve Outs

States with good carve-outs i.e., clear and appropriately comprehensive exemptions:

- Virginia Consumer Data Protection Act. Va Code **§ 59.1-576.**
- Connecticut Data Privacy Act, **Sec. 42-517**.
- Kentucky Consumer Data Protection Act, Section 2(2).
- RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT, Section 6-48.1-3 (d)-(f).
- Tennessee Information Protection Act, Section 47-18-3210 (a).

States with problematic carve-outs i.e., narrow or qualified or confusing exemptions:

- California Consumer Privacy Act, Section 1798.146(a)
  - applies to PHI that is "collected by" a covered entity or business associate, and so potentially not to other types of PHI (e.g., PHI accessed, received, transmitted or stored by such entities)
  - provides an entity-level exemption for HIPAA covered entities but not business associates
  - provides exemption for data used for research, but only if the research is conducted "in accordance with" applicable ethics, regulations and guidelines, and so effectively conditioning the exemption on whether California believes the research is being conducted in accordance with these requirements.
  - Applies to "personal information", which by definition excludes de-identified information, but then imposes conditions/requirements related to de-identified data, effectively regulating it.
- Delaware Personal Data Privacy Act
  - The law carves out PHI (not HIPAA entities), but then muddles it by adding an additional carve-out that states that it does not apply to "Information to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a Covered Entity or when provided by or to a Business Associate pursuant to a Business Associate Agreement with a Covered Entity." This exemption suggests that certain types of PHI are carved out only when used for certain purposes, thus potentially unintentionally limiting the carve-out for PHI.

HTI Hill Briefing Suggested Pre Reads

- HTI Response to Privacy Working Group
- Surveying the Landscape of Computable Consent | Healthcare Innovation
- Texas sues HHS over rule that limits access to reproductive health information by law enforcement | Healthcare Trust Institute
- US State Privacy Legislation Tracker
- Federal Trade Commission Chairman Andrew N. Ferguson Letter on 23andMe Bankruptcy Impact to Consumers