MARYLAND
Health Care
Commission

Patient Generated Health Data

A Closer Look at Privacy and Security Risks, the Current State of Health Care Cybersecurity, and State-Level Protections

DECEMBER 2022

Overview

- Use of direct-to-consumer health technologies (or third-party applications) is a rapidly growing sector that presents unique pathways to help consumers better manage their health and participate in their health care
  - Empowers patients to capture, use, and share health-related data (e.g., activity levels, symptoms, lifestyle choices); also referred to as "patient generated health data or PGHD"
- If these technologies are not integrated as part of a health care system, then the vendor does not have to meet HIPAA or HITECH guidelines, thus creating critical gaps in privacy and security protections particularly when consumers have very little understanding and control of how their health-related data is stored, accessed, and utilized
- Increasing awareness and strengthening privacy and security protections for PGHD is essential to reduce the risk of unauthorized access and cyber threats

What is Patient Generated Health Data?

- Defined as health-related data created and recorded by or from patients or family members/caregivers outside of a clinical setting
- Distinct from data generated in clinical settings in two ways:
  - Patients are primarily responsible for capturing or recording these data
  - Patients decide how to share or distribute these data to providers and others

Benefits

- Supplementing PGHD with clinical information from an electronic health record system provides a more comprehensive view of a patient’s current and ongoing health
- Expands providers’ knowledge about patients outside of clinical encounters
  - Increases visibility into patient adherence to a treatment plan
  - Enables timely interventions before a costly care episode

PGHD Risks

Current Landscape

- Privacy and security protections differ across consumer health technologies that maintain and transmit PGHD
- In many instances, PGHD is not protected by HIPAA, presenting risks to consumers who may intentionally or unintentionally share their health-related data
  - HIPAA only extends protections to protected health information (PHI) created, received, or maintained by or on behalf of covered entities (CEs) and business associates (BAs)
- Technologies that lack HIPAA-equivalent protections can result in:
  - Selling or sharing PGHD without users' consent or knowledge
  - Responding differently to a breach
  - Re-identifying PGHD (if proper security measures to de-identify the data are not in place)

Health Care Cybersecurity

Current State

- An increase of health care data breaches is due to an evolving cyber threat landscape
  - Persistent threats come from nation states and criminal financial scammers
- Cyber-attacks typically rely on techniques that interrupt business operations, leak confidential information, and compromise large volumes of data
  - Ransomware is the prominent root cause of breaches
- Safeguarding technology is a data, systems, and patient safety issue
- Cyber risk management – a key component of a broader business strategy to address cyber threats and strengthen overall security posture

A Closer Look at Breach Trends*

A Snapshot of 2018-2021

BREACH OCCURENCES

Nationally, growth in reported breaches have increased from 2018-2021 **(25%)**, but year-over-year growth rate is decreasing: **38%** (2018 to 2019), **31%** (2019 to 2020), **8%** (2020 to 2021)**

RECORDS

Total records compromised decreased for **Maryland (-19%);** the nation experienced an increase **(48%)**

BREACH TYPE

Hacking/IT incidents remain the leading breach type in 2021 **(81% Maryland | 74% nation)**

*Notes: *Data obtained from the U.S. Department of Health and Human Services, Office for Civil Rights public use file; breach growth*
*** 2018-2021 growth calculated using compound annual growth rate, a measure of growth over a specified period longer than one year; year-over-year growth calculated using percent change, the difference between an old and new value.*

Key Hacking/IT Trends

2018-2021

- Year-over-year growth for hacking/IT incidents has slowed in the nation: **46%** (2018 to 2019), **32%** (2019 to 2020), **14%** (2020 to 2021)*

- **Phishing** is the most common point of compromise for about **71%** of hacking/IT incidents

- For the health care industry, cyberattacks that rely on **ransomware** for potential monetary gain have almost doubled, increasing from **34%** in 2020 to **66%** in 2021

*Notes: *Year-over-year growth calculated using percent change, the difference between an old and new value.*

State-Level Legislation

Addressing Privacy and Security Gaps

Current Landscape

- To reduce the risk of unauthorized access and cyber threats, states are introducing bills aimed at protecting health-related data that falls outside the bounds of HIPAA
- In general, privacy provisions give consumers the right to know how and with whom their data is used, shared, or sold and the right to opt-in, opt-out, or restrict the selling and sharing of personal information; security provisions require consumer health technology vendors to implement specific security standards
- Twelve states (AZ, CA, CO, CT, FL, KY, MD, NV, UT, VA, VT, WY) have passed legislation since 2018
  - Four new states passed legislation during the 2022 legislative session (CT, KY, MD, WY)
  - Seven states have laws specific to genetic data

Notes: At least 29 states and the District of Columbia proposed consumer privacy bills in 2022 or carried over legislation from 2021, approximately 22 states (including Maryland) have breach notification laws that include health information in their definition of personal information; at the federal level, the Health Breach Notification Rule requires entities not covered by HIPAA (i.e., personal health record vendors and related entities) to inform consumers about unauthorized disclosures of their PHI. The Federal Trade Commission (FTC) is tasked with enforcement of the Health Breach Notification Rule.

Genetic Data

- AZ, CA, FL, KY, MD, UT, WY have enacted genetic data privacy laws
- Direct-to-consumer genetic testing companies provide services to make predictions about health, provide information about common traits, and offer clues about a person’s ancestry
    - Consumers send the company a DNA sample and receive their results directly from a secure website or in a written report
    - About 62% of consumers use third-party applications to interpret the raw data for both genealogy and health purposes

More Information

- State-level protections for PGHD and genetic data were identified through a legislative scan conducted by MHCC
- A findings summary overviewing legislation by state (enacted 2018-2022) is available at: mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_PGHD_Legislative_Table_20211201.pdf

Sources

- American Hospital Association Center for Health Innovation*, The Importance of Cybersecurity in Protecting Patient Safety*. www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety.

- Healthcare Information and Management Systems Society, 2021 HIMSS Healthcare Cybersecurity Survey, 2022. www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf

- ONC, *What Are Patient Generated Health Data?* January 2018. www.healthit.gov/topic/otherhot-topics/what-are-patient-generated-health-data.

- ONC, *What Are PGHD?* www.healthit.gov/sites/default/files/onc_pghd_final_white_paper_infographic.pdf.

- ONC*, Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024,* January 2018. www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.

- Maryland Health Care Commission*, Health Care Data Breach Trends, 2018-2021.* October 2022. mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Health_Care_Data_Breach_Trends.pdf

Sources *(continued…)*

- MedlinePlus, *What is direct-to-consumer genetic testing?* medlineplus.gov/genetics/understanding/dtcgenetictesting/directtoconsumer/#:~:text=Customers%20send%20the%20company%20a%20DNA%20sample%20and,provider%20or%20health%20insurance%20company%20in%20the%20process.
- Moscarello, T., Murray, B., Reuter, C.M. et al. *Direct-to-consumer raw genetic data and third-party interpretation services: more burden than bargain?* Genet Med 21, 539–541 (2019). doi.org/10.1038/s41436-018-0097-2.
- National Conference of State Legislatures, *2021 Consumer Data Privacy Legislation*. www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx.
- Security Magazine, *Concerned about Nation State Cyberattacks? Here's How to Protect your Organization*, March 2020. www.securitymagazine.com/articles/91889-concerned-about-nation-state-cyberattacks-heres-how-to-protect-your-organization.
- Sophos, The State of Ransomware in Healthcare 2022, June 2022. news.sophos.com/en-us/2022/06/01/the-state-ofransomware-in-healthcare-2022/.
- U.S. Department of Health & Human Services, *Health Sector Cybersecurity Coordination Center*, 2020: A Retrospective Look at Healthcare Cybersecurity, February 2021. www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.