1touch.io

Healthcare Data Security and Privacy

EVERYTHING YOU NEED TO KNOW

With elevating data breaches and regulatory scrutiny, data privacy and security have become a significant concern for healthcare providers and insurers. Here are 10 things you need to know about data privacy and security in healthcare.

HIPAA

1. The Health Insurance Portability and Accountability Act, designed to protect healthcare information security and confidentiality, was enacted in 1996.

2. The law is divided into Title I, which focuses on portability, and Title II, which focuses on administrative simplification. The portability portion of the law was put in place to ensure individuals can carry health insurance from one job to another. Title II focuses on how healthcare information is received and sent, and the maintenance of privacy and security.

3. HIPAA regulations apply to all healthcare providers, health plans, and healthcare clearinghouses. Protected health information includes the following:
    - Names
    - Birth dates, death dates, treatment dates, admission dates, and discharge dates
    - Telephone numbers and other contact information
    - Addresses
    - Social Security numbers
    - Medical record numbers
    - Photographs
    - Finger and voiceprints
    - Any other identifying numbers

4. Under the HIPAA privacy rule, patients have several rights, including:
    - The right to receive notice of privacy practices of any healthcare provider, plan or clearing house
    - The right to see their protected health information and receive a copy
    - The right to request changes to their records to correct errors or add information
    - The right to have a list of those their protected healthcare information has been disclosed to
    - The right to request confidential communication
    - The right to complain

Data Breaches in 2020 and Beyond

5. By the end of 2020, it's expected that security breaches could cost healthcare companies $6 trillion.
(Source: PhoenixNAP)

6. The healthcare industry is expected to spend around $65 billion on cybersecurity between 2017 and 2021.
(Source: HERJAVEC GROUP)

7. The healthcare industry is expected to spend around $65 billion on cybersecurity between 2017 and 2021.
(Source: HERJAVEC GROUP)

Top Data Breaches in the News

8. AMCA data breach: 25 million patients, investigation ongoing

In early May 2019, an 8-K filing with the Securities and Exchange Commission revealed billing services vendor American Medical Collection Agency had been hacked for eight months between August 1, 2018 and March 30, 2019. So far, up to 12 million patients from Quest Diagnostics were affected. Up to 7.7 million LabCorp patients were also potentially impacted, as well as 422,000 patients of BioReference. Recently, two more covered entities have been added to the tally: PenobscotCommunity Health Center in Maine with 13,000 affected patients, and Clinical Pathology Laboratories with 2.2 million patients.

9. Dominion National: 2.96 million patients

Insurer Dominion National reported a nine-year hack on its servers, which potentially breached the data of 2.96 million patients.

10. Elite Emergency Physicians (Formerly known as Elkhart emergency physicians): 550,000 patients

The provider, now known as Elite Emergency Physicians, was included in a massive security incident involving the improper disposal of patient records, including records from its Elkhart Emergency Physicians.

HIPAA vs. GDPR

	HIPAA	GDPR
Health Data in Space	Individually Identifiable Health Information (IIHP), relating to individual health (physical or mental), provision of care or payment for provision of care, when the IIHP is held or transmitted by a regulated entity or its business associate.	"Personal data" which includes direct or indirect identifiers and "expresses the physical, physiological, genetic, commercial, cultural or social identity" of individuals. Health data is a special category with heightened protection.
Regulated Entities	Health plans, health care providers, and health care clearinghouses Business associates - A person or organization performing functions on behalf of (or providing services to) a CE.	Controller - Any person or organization which determines the purpose or means of storing personal data. Processor - person or organization processing data on behalf of the controller.
Consent	Allows disclosure of some PHI for "treatment purposes" without the consent of the individual.	Explicit consent is mandatory for the processing of personal health data (which falls under sensitive data). However, the data may be processed without consent if it meets one of the conditions of processing in Article 9 of the GDPR and a legal basis applies.
Right to be forgotten	HIPAA does not grant this right	Individuals have the right to be forgotten (or to have their data deleted upon request)
Data breaches	Organizations must protect PHI and limit disclosure under the HIPAA Privacy Rule. Covered entities must also notify affected individuals of security breaches. If more than 500 people are affected, both the affected individuals and the Department of Health must be informed within 60 days.	The Supervisory Authority must be notified within 72 hours. Affected persons must also be notified.

What can companies do to secure customer data?

Data is a hot commodity, and healthcare data even more so. Healthcare providers need to invest in a sustainable data discovery solution for privacy and security. This is where 1touch.io comes in - 1touch.io's network-centric approach helps discover data origin, where it traveled, and how many copies of the data exist. 1touch.io provides a centralized view of data with a master catalog, using dynamic entity extraction with Natural Language Processing for data discovery from both structured and unstructured sources.

Our AI-based engine is fast, scalable, and delivers accurate information on any identified data subject. If sensitive data moves from a secured location to an unsecured location, 1touch.io can generate an alert to notify the DPO to take appropriate action.