BigID

Healthcare Regulations Cheat Sheet

Table of Contents

HIPAA: The Federal Standard for Healthcare Regulations in the U.S 3

Other Regulations Specific to the Healthcare Industry 4

HITECH 4

HITRUST 4

GINA 4

Interoperability and Patient Access 5

Hospital Price Transparency Rule 5

MACRA 5

U.S. State-specific Healthcare Laws 6

State-specific laws 6

CCPA 6

GDPR 6

How BigID Helps Healthcare Organizations Manage and Protect Their Data 7

HIPAA: The Federal Standard for Healthcare Regulations in the U.S.

The Health Insurance Portability and Accountability Act (HIPAA) has been the cornerstone of healthcare compliance in the U.S.since 1996. The act regulates the way health organizations collect, process, share, and maintain sensitive patient information called PHI — or "protected health information."

HIPAA applies to health care providers, health plans and insurers, health care clearinghouses, and businesses associated with health organizations — all of whom are termed "covered entities" under the law.

The regulation grants individuals rights over their health information and requires companies that handle PHI or electronic PHI (ePHI) to maintain specific privacy practices and security measures to protect patient data.

> **HIPAA regulates the way health organizations collect, process, share, and maintain sensitive patient information called PHI — or "protected health information."**

Other Regulations Specific to the Healthcare Industry

HITECH

- Enacted in 2009 — 13 years after HIPAA — the Health Information Technology for Economic and Clinical Health (HITECH) Act broadens HIPAA's scope and increases penalties for noncompliance.
- HITECH was created to promote the use of health information technology and electronic health records (EHRs).
- HITECH tightens language and addresses loopholes in HIPAA to reduce risk around the new influx of patient data that EHRs created.

HITRUST

- Formerly known as the Health Information Trust Alliance, HITRUST creates a framework that helps companies achieve HIPAA compliance standards.
- HITRUST establishes the Common Security Framework (CSF), which supports companies in regulatory compliance and risk management. It coordinates standards set by multiple regulations, including HIPAA.
- All major healthcare payers in the U.S. require HITRUST CSF certification.

GINA

- The Genetic Information Nondiscrimination Act (GINA) was enacted in 2008 to prohibit employers from requiring employees to disclose any of their health information — including genetic data, biometric information, or family medical history.
- GINA also prevents employers from disclosing or discriminating on the basis of employee health information.
- Under GINA, health insurance companies are also not allowed to use or disclose genetic data for underwriting purposes.

Other Regulations Specific to the Healthcare Industry

Interoperability and Patient Access

- As part of the Centers for Medicare and Medicaid Services' (CMS') commitment to the 21st Century Cures Act, the Interoperability and Patient Access Rule — set to go into effect in July 2021 — will improve patient access to health information, enhance interoperability, and boost innovation.
- Under the Interoperability and Patient Access Rule, the CMS regulates Medicare Advantage (MA), Medicaid, the Children's Health Insurance Program (CHIP) — and Qualified Health Plan (QHP) issuers on Federally Facilitated Exchanges (FFEs).

Hospital Price Transparency Rule

- In effect since January 2021, the Hospital Price Transparency rule helps consumers improve their understanding of costs related to healthcare.
- To address the categories of Hospital Price Transparency and Transparency in Coverage, the Centers for Medicare and Medicaid Services (CMS) requires that hospitals post their standard charges prominently on a publicly available website.
- The rule enables consumers to access real-time price information and know how much treatment will cost them.

MACRA

- Enacted in January of 2017, the Medicare Access and CHIP Reauthorization Act (MACRA) addresses how the federal government pays physicians.
- Established by the Centers for Medicare and Medicaid Services (CMS), MACRA replaced the sustainable growth rate (SGR) model with the Quality Payment Program (QPP).
- QPP emphasizes value-based payment over volume of service, connecting medical reimbursements to improved care and patient outcomes — while lowering costs.

U.S. State-specific Healthcare Laws

State-specific laws

- Every U.S. state and D.C. have laws that affect organizations in healthcare. These laws have slight differences, many areas of overlap. They include privacy and confidentiality protections — and regulate the collection, processing, and disclosure of patient health data in order to protect it
- State-specific regulations also include data breach notification laws and unfair or deceptive practices statutes.

CCPA

- The California Consumer Privacy Act (CCPA) gives California consumers rights over the data collected about them and requires that companies operating in the state or handling the data of California residents provide several safeguards for personal data.
- While CCPA exempts PHI that is covered by HIPAA, it regulates other consumer data that healthcare organizations collect, process, share, and maintain.

GDPR

- The European Union's General Data Protection Regulation (GDPR) became enforceable under EU law on May 25, 2018 — with the aim of granting EU citizens control over their personal data. GDPR creates a set of data privacy and protection rules for anyone who does business in Europe or processes the data of European citizens.
- The most important provisions for healthcare under GDPR include the right to access, which allows data subjects access to their information; the right to data portability, which permits data subjects to transfer their health data to another provider; and the right to be forgotten, which allows them to request termination and/or deletion of health data processing.

How BigID Helps Healthcare Organizations Manage and Protect Their Data

Using next-generation machine learning that goes beyond regular expressions and pattern matching, BigID enables health organizations to discover, map, tag, catalog, and take action on all of their sensitive patient information.

No matter what type of data you have or where it lives across the enterprise — on-prem, in the cloud, structured, unstructured, at rest, in motion, and more — BigID helps you classify, manage, and protect it to go beyond compliance requirements and unlock the most value across your organization.

Schedule a demo to discover all the ways BigID's data intelligence platform solution helps you know your data, take action on your data, and unlock more value from your data.

> **BigID enables health organizations to discover, map, tag, catalog, and take action on all of their sensitive patient information.**