FORTRA

US Health Insurance Portability And Accountability Act (HIPAA)

Protecting electronic protected health information

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 introduced national standards in the United States for the handling of electronic health care data. HIPAA was designed to address systemic inefficiencies and increase the effectiveness of the US health care system through the establishment of policy, standards and requirements addressing the electronic transmission of Personal Health Information (PHI). By doing so, fraud, waste and abuse could be identified and corrective actions undertaken.

To mitigate this risk, Congress introduced Federal privacy protection standards into HIPAA. Over subsequent years, the Privacy Rule, Security Rule, Enforcement Rule and then final Omnibus rule including Breach Notification Rules were introduced. These rules mandate standards of handling and protection for individually identifiable health information; PHI.

HIPAA defines health information as any information, whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual. This includes the provision for an individual's past, present, or future payment for health care. Examples would include name, address, date of birth or social security number.

Electronic Protected Health Information (ePHI) includes any individually identifiable health information, where "identifiable" refers not only to data explicitly linked to a particular individual (identified information), but also includes health information with data items that could reasonably be expected to allow individual identification.

HIPAA At A Glance

What Is HIPAA?
Legislation to encourage the use of electronic healthcare data, and mandate it is handled and secured appropriately

How Is HIPAA Regulated?
Since September 2009, data breaches involving the health information of more than 500 people are required to be reported promptly to the U.S. Department of Health and Human Services (HHS), major media outlets, and each individual affected by the breach

What Is A "Covered Entity"?
Covered entities are health care providers, health plans, health care clearinghouses, and those who carry out tasks on their behalf

To ensure HIPAA compliance, Covered Entities must specifically:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit,

- Identify and protect against reasonably anticipated threats to the security or integrity of the information,

- Protect against reasonably anticipated, impermissible uses or disclosures and,

- Ensure compliance by their workforce.

Additionally, there are both 'Required' and 'Addressable' controls specified by the HIPAA Security Rule that the organization must consider:

- **Administrative Safeguards** - Policies and controls designed to achieve, maintain and demonstrate compliance

- **Physical Safeguards** - Controls governing the access to hardware, software and user environments that process, store or transfer health information

- **Technical Safeguards** - Provide controls and their documentation ensuring the integrity and confidentiality of the data, the networks and users of health information

Boldon James Classifier enables an organization to mark ePHI, both visibly and via metadata, which is embedded in the DNA of the file. Classifier can content-check files identifying ePHI and mandating or suggesting a classification accordingly.

Intelligent rules can leverage this classification to ensure that data identified as ePHI is not disseminated, accidentally or with malicious intent, by checking emails with unauthorized recipients. Classifier also drives 3rd party solutions, helping to address compliance to the Administrative Safeguards. Administrative Safeguards expressly state that organizations must safeguard Information Access Management by "implementing policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient's role (role-based access)."

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports compliance with HIPAA by:

- Applying visual markings and metadata to documents containing ePHI supporting special handling requirements and application of downstream controls to include:

  - Data Loss Prevention (DLP)

  - Encryption

  - Retention and deletion

  - Insider Threat – User and Entity Behavior Analytics (UEBA)

  - Fostering cloud collaboration solutions via Cloud Access Security Broker (CASB)

- Increasing users awareness about data sensitivity with visual labels

- Alerting or preventing users when they attempt to send messages that include sensitive information outside of the organization

Don't Delay Your Preparations

HIPAA compliance is vital for working in or contracting for the healthcare industry in the US, but this need not seem a barrier to working in this field. With the application of Boldon James best-of-breed classification, marking and managing ePHI is simplified, easing compliance.

Data classification embeds a culture of compliance by involving users in identifying, managing and controlling regulated data, while automating parts of the protection process to enforce rules and policies consistently.

As you look to comply with regulations such as HIPAA, classifying data as a first step will enable the protection strategy and solutions you implement to be built around the types of data you have, and the levels of security they require.

FORTRA

Fortra.com