HIPAA/HITECH and the Value of DataKeep

Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to improve the health insurance system in the United States by providing individuals with the ability to control their own health information. It set rules for health care providers and insurance companies about who can look at and receive your health information including the individual's right to get a copy, make sure it is correct, and know who has seen it. HIPAA ushered in a new era for data privacy by encouraging a move from paper to a more shareable electronic health records (EHR) format and set a requirement (Sec. 262 Administrative Simplification) for the U.S. Department of Health and Human Services (HHS) to define national standards for electronic health care transactions.

HHS published Code of Federal Regulations Title 45 (45 CFR) Part 160 and 164 containing the Privacy and Security Rules. The Privacy Rule established minimum standards for protecting the electronic transaction of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers. The Security Rule established minimum standards to protect an individuals' electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity. It also defined the appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

The Health Information Technology for Economic and Clinical Health (HITECH) Act expanded upon the privacy rights clauses introduced with HIPAA by defining new rules for reporting breaches of unsecured ePHI and significantly increasing financial penalties for HIPAA violations. While HIPAA was enacted on August 21, 1996, it required HHS to issue regulations governing the privacy of health information if Congress did not enact specific privacy legislation within three years of the passage of HIPAA. In response, HHS created the Privacy Rule and Security Rule, often referred to as the Administrative Simplification provisions. These regulations went into effect on April 14, 2003 for the HIPAA Privacy Rule, and April 20, 2005 for the HIPAA Security Rule. The HITECH omnibus for extended breach notification and penalties went into effect, January 25, 2013.

HIPAA, the Administrative Simplification and HITECH are very complex documents with many sections outside the scope of what a data-centric solution like DataKeep can impact, so the focus here is on the specific requirements related to data protection. An organization's answer to HIPAA/HITECH compliance will most likely be comprised of documented processes, multiple software products and services that may include considerable professional consulting engagements. This overview presents areas where DataKeep can help support certain requirements of HIPAA/HITECH. In reviewing where DataKeep supports HIPAA/HITECH we will break out sections from the HIPAA Administrative Simplification Regulation, 45 CFR Parts 160, 162, and 164, as amended through March 26, 2013.

GENERAL PROVISIONS – ADMINISTRATION AND FINES

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

- **160.103 Definitions**
- **160.404 Amount of a civil money penalty.**

PART 164 – SECURITY AND PRIVACY

SUBPART C – SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

- **164.306 Security standards: General Rules**
- **164.308 Administrative Safeguards**
- **164.310 Physical Safeguards**
- **164.312 Technical Safeguards**

PART 164 – SECURITY AND PRIVACY

SUBPART D – NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

- **164.404 Notification to Individuals**
- **164.406 Notification to the Media**
- **164.408 Notification to the Secretary**

GENERAL PROVISIONS – ADMINISTRATION AND FINES

The Privacy Rule applies to health plans, healthcare clearinghouses, and to any health care provider who transmits health information in any form. Failure to provide appropriate safeguards can result in fines being assessed depending upon the degree of 'willful neglect' and lack of corrective actions.

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENT

160.103 Definitions

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   (i) That identifies the individual; or
   (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information means individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   (i) Transmitted by electronic media;
   (ii) Maintained in electronic media; or
   (iii) Transmitted or maintained in any other form or medium.

160.404 Amount of a civil money penalty

(b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

2. For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty—
   (i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, in the amount of less than $100 or more than $50,000 for each violation; or in excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
   (ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, in the amount of less than $1,000 or more than $50,000 for each violation; or in excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
   (iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, in the amount of less than $10,000 or more than $50,000 for each violation; or in excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
   (iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30- day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, in the amount of less than $50,000 for each violation; or in excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

RULES RELATED TO DATA-CENTRIC PROTECTION

PART 164 – SECURITY AND PRIVACY

SUBPART C – SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

164.306 Security standards: General Rules

(a) General requirements. Covered entities and business associates must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
4. Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
   (i) The size, complexity, and capabilities of the covered entity or business associate.
   (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
   (iii) The costs of security measures.
   (iv) The probability and criticality of potential risks to electronic protected health information.

164.308 Administrative Safeguards

Includes the establishment of processes and procedures that a covered entity will use to implement the security program including: Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review. A privacy official responsible for the development and implementation of the policies and procedures must be designated.

DataKeep for Administrative Safeguards

(164.308(a)(4)) DataKeep builds upon standard directory services capabilities (Active Directory or LDAP) to provide a second level of file or volume access control.

(164.308(a)(5)) DataKeep supports a least-privileged access (LPA) approach, privileged access management (PAM), a separation of product deployment and security rules, and it creates auditable logs for every successful or attempted ePHI access.

(164.308(a)(7)) DataKeep can also create and maintain retrievable exact copies of electronic protected health information stored within one or more object storage repositories either on-premises or within one or more public clouds.

164.310 Physical Safeguards

Focuses on physical access to ePHI irrespective of its location or media format. ePHI could be stored on servers which located within the premises of the HIPAA covered entity or within a remote data center including public cloud environments.

DataKeep for Phsyical Safeguards

(164.310(d)(1)) DataKeep protects data stored both on-premises and in-cloud repositories located within secure environments. Encryption keys can be controlled by the data owner including creation, rotation and revocation (cryptographic shredding) to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. DataKeep can also create a retrievable, exact copy of electronic protected health information, when needed, before movement of any IT equipment.

164.312 Technical Safeguards

Concern the technology that is used to protect ePHI and provide access to the data. ePHI – whether at rest or in transit – must be encrypted to NIST standards once it travels beyond an organization´s internal firewalled servers. Data must be rendered unreadable, undecipherable and unusable to all unauthorized recipients.

DataKeep for Technical Safeguards

(164.312(a)(1)) DataKeep begins protecting data from the point at which it's created in an application – such as EHR – through to when it's stored in an encrypted data repository. It applies AES 256 encryption and is certified to meet FIPS 140-2 requirements. All stolen or lost data is useless to external parties.

(164.312(b)) DataKeep also logs every successful or unsuccessful access to protected data and can forward this data to a security analytics tool for automated analysis.

RULES RELATED TO BREACH NOTIFICATIONS

PART 164 – SECURITY AND PRIVACY

SUBPART D – NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

164.404 Notification to Individuals

1. General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.
2. Breaches treated as discovered. A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

164.406 Notification to the Media

(a) Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach notify prominent media outlets serving the State or jurisdiction.

(b) Timeliness of notification. A covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

164.408 Notification to the Secretary

(a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information notify the Secretary.
(b) Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall provide the notification required in the manner specified on the HHS Web site.
(c) Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification in the manner specified on the HHS web site.

DataKeep for Notifications

A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. Following a breach of unsecured ePHI, covered entities must inform affected individuals, the HHS Secretary, and sometimes even the media; however, notification is only required if the breach involved unsecured ePHI (HITECH 13402 (h)(2)).

Covered entities and business associates do not have to report secured ePHI when they can produce documentation to demonstrate a low probability of compromise based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification (164.402 (2)(i))
2. The unauthorized person who used the protected health information or to whom the disclosure was made (164.402 (2)(ii))
3. Whether the protected health information was actually acquired or viewed (164.402 (2)(iii))
4. The extent to which the risk to the protected health information has been mitigated (164.402 (2)(iv))

The security offered by DataKeep address all four of these conditions. As a first step in applying data protection, access control policies are established based on a data identification or classification scheme. Those that are encrypted have no chance of providing any useable identifiers. DataKeep agent technology tracks all activity at the file or volume levels recording network metadata identifying the source and nature of the access. The application of AES-256 technology assures that any risk of unsecured ePHI disclosures has been mitigated.

HIPAA ePHI Data Protection by Design and Default

DataKeep supports covered entities in relation to data protection requirements under HIPAA and can help avoid breach notification requirements by protecting ePHI with access management, encryption and monitoring. Enterprises can quickly and easily apply this software-only solution to data within their network environments, even including datasets migrated to a cloud environment for long-term storage. Other organizations may prefer to select a managed services provider (MSP) to help with the management of data-centric protection from the broad network of SecurityFirst partners.

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

DataKeep™, by SecurityFirst, secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency and enable prompt recovery of archived data in the event of a ransomware attack.

SecurityFirst™
Protecting Critical Data

For a product demonstration
or more information call
1-888-884-7152
securityfirstcorp.com