HIPAA

Educational Briefing for IT Professionals

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) addresses several significant issues for the health care industry, including insurance portability, fraud and abuse issues, and notably, privacy and security of health information. Congress enacted HIPAA in 1996, and the legislation's focus on protecting the privacy and security of health information has had a resounding impact on modern health care delivery.

Why is HIPAA a key issue for providers?

Patients often divulge sensitive information to clinicians, and providers must assume this responsibility of privacy protection with integrity or face reputational and financial consequences. HIPAA compliance is again a major focus for providers because of meaningful use mandates – providers face new challenges securing electronic protected health information (PHI) as they transition from paper to electronic health records (EHR).

How does HIPAA work?

Significant HIPAA Amendments

The Privacy Rule
(2002)

- Governs use and disclosure of PHI by covered entities (CEs)
- Provides individuals with certain rights to access their PHI
- Mandates CEs to create HIPAA privacy compliance programs

The Security Rule
(2003)

- Requires the implementation of administrative, physical, and technical safeguards (e.g., access controls, and physical security) to protect the confidentiality, integrity, and availability of electronic PHI

The Omnibus Final Rule
(2013)

- Increases obligations, enforcement, and financial penalties for non-compliance
- Expands HIPAA Security Rule to business associates (BAs)
- Finalizes breach notification obligations

The HIPAA Privacy Rule governs when a covered entity (CE) may use or could disclose PHI, establishes certain rights individuals have to access their PHI, and sets forth administrative requirements that must be implemented to ensure compliance. The HIPAA Security Rule sets forth the administrative, physical, and technical safeguards a CE and a business associate (BA) must have in place to protect the confidentiality, integrity, and availability of electronic PHI. Lastly, the Omnibus Final Rule expands the Security Rule to all parties that create, receive, maintain, or transmit PHI during the course of providing a service to a CE. This amendment also requires a BA agreement to be in place between the CE and BA to ensure the BA provides reasonable assurances that it will protect the privacy and security of the PHI.

Questions That Hospital Executives Should Ask Themselves

1. What safeguards are in place at my hospital to secure patients' PHI?
2. How are meaningful use mandates affecting my hospital's PHI risk management and data sharing protocols?
3. How does my hospital or health system respond to impermissible uses or disclosures of PHI?

March 2016

Sources: Advisory Board Research and Analysis; Department of Health and Human Services.

How does HIPAA affect providers?

Clinical

HIPAA permits a CE to use or disclose PHI for treatment, payment, and health care operations without an individual's authorization. This means, for example, a provider can use PHI to diagnose and provide care to a patient and refer a patient to another provider as part of treatment, submit a claim for payment, and conduct quality improvement activities as part of health care operations without an individual's authorization. Other uses and disclosures, such as those required by law, disclosures to health oversight agencies, reporting adverse events to an FDA regulated entity, or using or disclosing PHI for research may be made without an authorization in certain circumstances, provided the requirements set forth in HIPAA are met. Overall, providers must be knowledgeable about the nuances of HIPAA, because the requirements related to use and disclosure of PHI are situational.

Financial

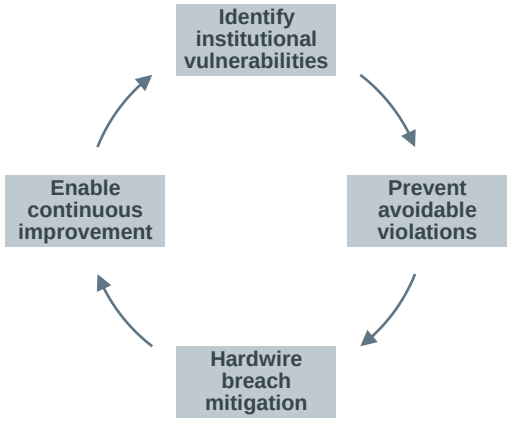
Under 2013's Omnibus Final Rule, financial penalties for HIPAA violations range from $100-50,000 per violation (i.e. each individual EHR compromised) depending on the circumstances, with a $1.5 million annual cap. The Omnibus Final Rule also impacts providers financially by expanding what types of PHI may be used for fundraising and enhancing opt-out provisions for patients uninterested in volunteering their PHI.

Operational

Providers must prioritize risk management to develop a culture of transparency and compliance. Managing sensitive data privacy and security risks requires a holistic approach to risk management because breaches are unexpected and can permeate an organization. Providers must emphasize risk management best practices – such as properly reporting sentinel events to leadership and governing agencies, and training and educating staff on HIPAA's legalities and significance – to minimize adverse events. At the same time, providers must also ensure they abide by HIPAA requirements that afford patients certain rights to access their PHI.

As providers use EHRs to fulfill meaningful use requirements, new HIPAA challenges will emerge, such as protecting cloud-based PHI, securing electronic data sharing, and enhancing current reporting and breach notification standards. Providers must also respond to ever-changing forces in the regulatory and IT environment such as the advent of Application Programming Interfaces (APIs). Ultimately, providers must safeguard electronic PHI as technology becomes more operationally integrated and new technologies affect how providers share PHI.

The Cycle of Risk Management



How might HIPAA affect IT?

Secure Electronic PHI
- PHI needs to be protected both physically (e.g., secured rooms for data servers) and technologically (e.g., encryption and firewalls).

Upgrade IT Infrastructure
- Ensure that the IT infrastructure is HIPAA compliant.

Communications Plan
- Prepare a plan to ensure a quick and effective response in the event of a breach or other security incident.

Additional Advisory Board research and support is available

If you would like more information on how HIPAA is impacting meaningful use planning, please contact your institution's Dedicated Advisor. To see how providers are operationalizing risk management, please view our HIPAA Implementation Toolkit.

Sources: Advisory Board Research and Analysis; Department of Health and Human Services.