FAQ's About 4 Major Legislative Regulations:

How Your Business May Be Affected

In this guide

In this e-guide:

Complying with major legislative regulations is something that your IT team surely knows they may one day encounter. However, when it gets down to the nitty-gritty, IT operations are sometimes unexpectedly affected by major audit regulations. Do these regulations affect you and does your IT team need to comply? What is the IT team's role in ensuring compliance with the audit? What are the penalties for non-compliance?

This comprehensive guide walks readers through these FAQ's about some of the most well-known, but also most impactful audit regulations such as Sarbanes-Oxley, HIPPA and the HITECH Act.

In this guide

What is the impact of a compliance audit on IT operations

http://searchcompliance.techtarget.com/feature/FAQ-What-is-the-impact-of-a-compliance-audit-on-IT-operations

Complying with the increasing number of regulations has made leveraging IT essential. That's particularly true in the automation of processes to handle the information in an organization's possession.

As requirements grow, systems that both facilitate compliance and demonstrate to auditors that standards for security and data protection have been met are an increasingly critical area of IT operations. Learn more in this FAQ.

What is a compliance audit?

According to WhatIs.com, a compliance audit is a "comprehensive review of an organization's adherence to regulatory guidelines." This review generally

surveys internal systems, such as user access controls and security policies, to test whether the organization is meeting its regulatory obligations. Most reviews are conducted by independent, external parties, such as government auditors or consultants with IT expertise. Organizations are asked to demonstrate that they have policies and procedures in place for achieving compliance.

How are compliance audits different?

Not all audits are the same. Consider, for instance, a financial audit of a public company's quarterly results. Both compliance and financial audits involve reviews of internal control systems by independent parties, but the scope and subject of the reviews differ. A financial audit focuses primarily on controls related to accounting and financial reporting systems to determine whether the resulting financial statements are accurate, fair and complete. A compliance audit examines an organization's internal systems and IT controls more broadly to test whether a particular set of regulatory requirements is being met.

In this guide

What regulations require compliance audits?

Until recently, the concept of a compliance audit typically evoked the 2002 Sarbanes-Oxley Act (SOX). Officially entitled the U.S. Public Company Accounting Reform and Investor Protection Act, SOX pertains to all publicly traded companies. A growing body of federal law, however, requires audits of internal control systems to ensure compliance with regulations. Some laws are industry-specific, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), officially entitled The Financial Modernization Act. Additionally, there are industry-set standards that impose audit requirements, such as the Payment Card Industry Data Security Standard (PCI DSS).

Compliance audits are achieved in different ways depending on the regulations being enforced. The vast majority will involve an assessment of IT systems because such systems have become integral to compliance processes. Auditors typically meet with CIOs, chief technology officers and IT managers to discuss how these systems are secured and who has access to them. Auditors also request documents that demonstrate that an organization is meeting its regulatory requirements.

In this guide

Sarbanes-Oxley Act: A compliance audit evaluating conformity with the Sarbanes-Oxley Act requires a company to explain the process by which it generated the figures on its financial statements and how those numbers can be validated. Financial reporting processes at public companies generally rely on IT systems. As a result, the controls for those IT systems will be at the heart of an assessment of SOX compliance. The law requires reports on how effective the controls and procedures for financial reporting are, which means companies have to document and be able to demonstrate how the processes are secured and how well they work. Nonfinancial systems as well as financial systems may be evaluated in a compliance audit.

Learn more in this SOX FAQ.

PCI DSS: The challenges associated with PCI compliance and audits are quite different from those associated with the Sarbanes-Oxley Act. PCI DSS establishes very specific compliance measures, leaving little room for differing interpretations. Greg A. Nolann pointed out the difficulties an organization can confront in addressing both types of compliance challenges in "Seeking Compliance Nirvana," an article for the Association for Computing Machinery. "SOX and PCI address similar goals but take

approaches that are 180 degrees apart," he wrote. "SOX doesn't specify a standard; instead it says to use some other established methodology or set of practices. PCI, on the other hand, specifies exactly what you must do, who can do it, where it applies, and how to determine if you are compliant."

Learn more in this PCI DSS FAQ.

HIPAA: Health care providers that store or transmit electronic health records are subject to HIPAA requirements. The Center for Medicare & Medicaid Services, a division of the U.S. Department of Health and Human Services (HHS), provides a checklist of the kinds of information an auditor of HIPAA regulations requests. Experts recommend that an organization figure out which checklist items have been addressed and then prepare a statement that explains why they were or were not implemented to prepare for a HIPAA compliance audit. It is also important that you make a written policy for records management and retention available for review and have staff training up to date.

Who performs compliance audits?

Compliance audits are generally conducted by government auditors or contractors so that there is an independent, third-party certification made for an organization's adherence to relevant regulations. Some regulations, however, require internal as well as external audits. Under the Sarbanes-Oxley Act, for example, internal auditors assure that internal control systems are effective. Industry-established regulations can also require internal audits. Under PCI DSS, most merchants are required to bring in an externalQualified Security Assessor for a compliance audit. In a particular set of circumstances, some merchants can use an internal auditor instead.

Internal audits are sometimes conducted in preparation for external compliance audits. It is important to make sure policies and practices are up to date, enforced and documented. Since organizations should be prepared to turn over the documents at the auditors' request, they should be stored in noneraseable, nonrewriteable formats and located where they can be accessed easily and retrieved quickly.

In this guide

IT managers can prepare for audits by deploying information management tools, such as event log managers and change management programs, to make it easier to track and document internal controls and demonstrate compliance to auditors.

Preparing for a SOX audit can take hundreds of hours. Preparation requires reviewing information on the internal controls for financial data -- such as security, implementation, disaster recovery and change management -- and verifying the controls as well as the data.

What is the role of IT in a compliance audit?

After the introduction of numerous state data breach and protection laws, a central responsibility of IT is now to protect sensitive data within an organization. This responsibility encompasses keeping track of who can access the data and how. Given that IT systems are integral to financial reporting and other regulatory requirements, an assessment of the IT system's internal controls is also critical to a compliance audit. This applies not only to compliance audits that involve the Sarbanes-Oxley Act, but also to the Gramm-Leach-Bliley Act, HIPAA, HHS regulations and more.

In this guide

Effective compliance frameworks should be supported by IT systems that suit a particular organization and the relevant regulations. Document management, event log management software, change management software and other tools can help achieve compliance with regulations and facilitate compliance audits.

An organization's IT professionals now work closely with other sides of the business , such as finance, legal and internal audit, to meet compliance goals. IT professionals should also collaborate with these departments in preparing for a compliance validation and then helping during the auditing process.

What are the penalties for noncompliance?

Failure to comply with regulatory obligations -- which include compliance audits -- can result in fines and prison terms, depending on the area of noncompliance. Under the Sarbanes-Oxley Act, for instance, the destruction of relevant email can result in fines up to $5 million and 20 years imprisonment. Noncompliance with the GLBA can result in five years in prison, as well as fines.

In this guide

Regulations established by industry bodies such as the New York Stock Exchange or the PCI Security Standards Council do not include imprisonment for noncompliance but do impose fines.

Next article

In this guide

What is the impact of Sarbanes-Oxley on IT operations

http://searchcompliance.techtarget.com/feature/FAQ-What-is-the-impact-of-Sarbanes-Oxley-on-IT-operations

With the great impact Sarbanes-Oxley (SOX) has on IT operations, you need to stay informed on who it affects, what is required and what penalties are applied. Get key insights into how your organization should approach SOX mandates from these FAQs.

What is the Sarbanes-Oxley Act?

When former President George W. Bush signed the Sarbanes-Oxley Act into law July 30, 2002, he called its provisions "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt." SOX was enacted in response to high-profile financial scandals in which accounting errors and fraudulent practices resulted in the collapse of Enron and WorldCom. Sarbanes-Oxley was designed to protect shareholders and the general public from similar scandals, particularly with regards to criminal

In this guide

accounting in public companies. Compliance with SOX is administered by the Securities and Exchange Commission (SEC), which publishes requirements and sets deadlines for organizations to comply with them. The SEC provides up-to-date information about the Sarbanes-Oxley Act on its website.

When it comes to IT operations, the impact of Sarbanes-Oxley has been clear and far-reaching. In fact, the costs of complying with SOX have resulted in many companies choosing to go public outside the U.S. capital markets. As noted in "Sarbanes-Oxley Revisited" in *Reason Magazine*, however, "the SEC has continued to exempt nearly 5,000 smaller companies, with market capitalizations of less than $75 million, from SarbOx's orders to audit their financial control systems. That exemption is currently set to end in December 2009." When it does, SOX requirements will extend to the IT departments of many more public companies.

What is the role of IT in SOX compliance?

Compliance is now a deeply embedded aspect of corporate IT culture. Why? Sarbanes-Oxley regulations require that an audit trail of log files and all pertinent documentation must be retained for five years. SOX defines which

records are to be stored and for how long, focusing specifically on retention of audit and accounting records that relate to the generation of financial statement that will be submitted to shareholders and the SEC. Both paper and electronic versions of this documentation must be retained. SOX does not, however, specify how they are to be stored -- best practices for data protection, disaster recovery and storage management pertain. That means the impact of Sarbanes-Oxley can be felt by nearly every component of IT operations, including messaging, storage, virtualization and even networking, so long as financial data or activity occurs on them. In turn, IT must be able to produce electronic records of these audit trails for compliance audits.

Many enterprise IT shops use Control Objectives for Information and Related Technology (COBIT) as a reference framework for this work. COBIT is an open standard that defines requirements for the control and security of sensitive data. According to WhatIs.com's definition for COBIT, the standard "consists of an executive summary, management guidelines, framework, control objectives, implementation tool set and audit guidelines. Extensive support is provided, including a list of critical success factors for measuring security program effectiveness and benchmarks for auditing purposes."

In this guide

The IT departments of all public companies must be aware of the key requirements of SOX, including log management, backups and all relevant electronic communications. New platforms for communication enabled by Web 2.0 technologies like blogs, wikis and social networking are introducing all-new compliance headaches, as gigabytes of data are generated through messaging and sharing. If it pertains to finance and accounting, enterprise IT professionals must track and archive it for the inevitable visit by a compliance auditor looking for log files. Increasingly, compliance officers are using event log management software to track key moments where data enters or exits an enterprise, like email systems or the addition or departure of employees with access to sensitive financial data.

Who is affected by SOX compliance?

Anyone who administers systems that are relevant to financial or accounting data is affected by SOX. Many large enterprises have chosen to appoint chief compliance officers to coordinate the work of network administrators, database administrators and remote IT departments. SOX compliance has also forced substantial investment in human resources to maintain, organize and

In this guide

retain audit trails. These responsibilities are often passed on to the IT department.

SOX affects only publicly traded companies, unlike compliance regulations like the Payment Card Industry Data Security Standard or Health Insurance Portability and Accountability Act. As a result of the financial and legal penalties that noncompliance imposes, corporate executives have been active in pushing financial and IT departments towards compliance validation. Accounting departments have been able to use sophisticated financial software developed in the years since SOX passed to meet financial requirements. CIOs and chief technology officers are now usingevent log managers and governance, risk management and compliancesoftware to ease the burden of compliance. As SearchCompliance.com Senior News Writer Linda Tucci reported, however, for compliance management, GRC software may not be the answer.

What is generally required by SOX?

SOX regulations were written in the wake of massive accounting scandals at Enron, Worldcom and Tyco in the early years of the new millennium. As a

result, SOX compliance focuses squarely on the retention of audit trails, in the form of log files and work-papers, for any electronic records that contain, relate to or comment upon financial data. These work-papers and electronic audit trails may not be destroyed, altered or falsified. Revant audit trails must be retained and auditable for five years.

What are the penalties for noncompliance?

The consequences for noncompliance with SOX regulations are fines, imprisonment or both. The severity of the penalty varies with the infraction. Failure to maintain documents and documentation can result in up to 10 years in prison and/or fines. Destruction, alteration or falsification of records can result in up to 20 years in prison and/or fines. Defrauding shareholders of publicly held companies can result in up to 25 years in prison and/or fines.

Section 802 of the Sarbanes-Oxley Act describes these penalties in detail. Specifically:

"Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the

intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both." (Section 1519)

These penalties also pertain to destruction, alteration or falsification of records in federal investigations and bankruptcy (Section 1519) and destruction of corporate audit records (Section 1520).

SOX audit statements must be certified by the chief executive officer of the corporate entity. In situations where penalties are assessed, the leaders of the organization are typically held to account, not the IT managers who prepare the report. Ultimate repsonsibility for the accuracy of SOX compliance reports generally rests in the executive suite, not the server room.

Next article

In this guide

What is the impact of HIPAA on IT Operations?

http://searchcompliance.techtarget.com/feature/FAQ-What-is-the-impact-of-HIPAA-on-IT-operations

This FAQ guide describes the impact of the Health Insurance Portability and Accountability Act on IT operations, includes the guidelines that health care organizations must follow in order to meet compliance mandates, provides answers to frequently asked HIPAA questions and an overview of what penalties are involved. This is the essential toolkit for anyone involved in ITcompliance as it relates to HIPAA.

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996. There are two sections in HIPAA:

The first, Title I, provides protections for the health insurance coverage of people who lose or change jobs. HIPAA made changes to three areas in the

continuation coverage rules applicable to group health plans under the Consolidated Omnibus Budget Reconciliation Act of 1985 -- or COBRA -- each of which are described more extensively by the US Department of Labor atDOL.gov.

Title II is where organizations feel the impact of HIPAA on IT operations. It includes a section that deals with the standardization of healthcare-related information systems for electronic data interchange . These mandatory regulations all required extensive changes to the way that health providers conduct business.

Compliance with HIPAA is administered by the U.S. Department of Health and Human Services (HHS), which publishes requirements and sets deadlines for organizations to comply. HHS provides up-to-date information about HIPAA at HHS.gov.

What is generally required by HIPAA?

Compliance with HIPAA requires organizations to implement safeguards and security standards when electronically storing and transmitting personal health

information. HIPAA mandates standardized formats for all patient health, administrative and financial data. HIPAA also requires a unique identifier (essentially an ID number) for each healthcare entity, including individuals, employers, health plans and healthcare providers.

As the legislation was drafted, two additional rules were added to protect the privacy and safety of individuals' personal health information (PHI). These are called the Privacy Rule and the Security Rule. The Privacy Rule is the first comprehensive federal protection for the privacy of PHI, according to the National Institutes of Health (NIH). More information on the Privacy Rule can be found at PrivacyRuleandResearch.NIH.gov. The Centers for Disease Control and Prevention also offers guidance on the Privacy Rule and public health.

The Security Rule describes best practices organizations must adopt to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). The Security Rule contains three types of standards: administrative, physical and technical. These standards are wide-ranging and require the involvement of a broad mix of people, processes and technology for full compliance.

In this guide

HIPAA specifically requires that public companies or those that handle personal health information monitor or retain audit trails. To meet this requirement, event log management software (ELMS) is used to monitor change management and prepare for compliance audits at enterprises. ELMS is a key tool for IT administrators who must demonstrate to executives that an organization is prepared for a compliance audit.

Although wireless devices are not detailed in HIPAA's security rule, they must be viewed in the entire system for electronically storing and transmitting data.

Many IT departments find value in a third-party assessment of HIPAA compliance. The URAC (formerly the Utilization Review Accreditation Commission), the largest accrediting body for healthcare, will certify that a healthcare organization's operations are in compliance with HIPAA standards. The URAC provides an IT department with documentation and evidence of due diligence that support an organization's overall risk management efforts. As Robert N. Mitchell wrote for AdvanceWeb.com, the URAC has reported progress on HIPAA programs.

In this guide

Who is affected by HIPAA compliance?

The Security Rule applies to healthcare organizations that create, receive, maintain or transmit ePHI, including:

- **Healthcare providers**: Providers of medical or other health services or suppliers who transmit any electronic health information.
- **Health plans**: Individual or group plans, including employer-sponsored health plans, Medicare and Medicaid programs.
- **Healthcare clearinghouses**: Public or private entities that process healthcare transactions from a standard format to a nonstandard format or vice versa.
- **Medicare prescription drug card sponsors**: Any entity that offers an endorsed discount drug program under the Medicare Modernization Act.

As a result of the financial and legal penalties that noncompliance imposes, corporate executives have pushed financial and IT departments toward compliance validation. In the years since HIPAA's introduction, healthcare

organizations have developed a clearer picture of what practices will best protect themselves and patient information.

What is the role of IT in HIPAA compliance?

Compliance is now a deeply embedded aspect of corporate IT culture. Why? HIPAA requires that the privacy of health records be protected, wherever they reside or whenever they are moved. That means the impact of HIPAA can be felt by nearly every aspect of IT operations, including messaging, storage, virtualization and even networking, so long as electronic PHI (ePHI) records are stored within or transferred over them. In turn, IT must be able to produce evidence of the security of these systems for compliance audits.

Healthcare organizations must be able to demonstrate that they have standardized mechanisms for the security and confidentiality of all healthcare-related data. From an IT perspective, there are several general guidelines that entities must follow:

In this guide

- Ensure the confidentiality, integrity and availability of all ePHI, including the protection of patient privacy by encrypting medical records.
- Protect against reasonably anticipated threats or hazards to the ePHI the entity creates, receives, maintains or transmits.
- Deliver visibility, control and detailed auditing of data transfer.
- Protect against reasonably anticipated uses or disclosures of ePHI, including preventing the loss of confidential medical records via removable devices.
- Ensure that the organization's workforce complies with HIPAA and minimizes the threat of data being stolen for financial gain.
- Review security measures as needed to ensure reasonable and appropriate protection of ePHI.

Many enterprise IT shops use Control Objectives for Information and related Technology (COBIT) as a reference framework for this work. COBIT is an open standard that defines requirements for the control and security of sensitive data. According to WhatIs.com's definition for COBIT, the standard "consists of an executive summary, management guidelines, framework,

control objectives, implementation tool set and audit guidelines. Extensive support is provided, including a list of critical success factors for measuring security program effectiveness and benchmarks for auditing purposes."

The IT departments of all companies that handle PHI must be aware of the key requirements of HIPAA, including log management, backups and the security of electronic communications. IT departments also approach HIPAA compliance through PHI flow analysis, training, policy and procedure refinement, risk analysis and self-assessment.

The impact of HIPAA can also be felt on Web 2.0 technologies like blogs, wikis and social networking. Such platforms are introducing all-new compliance headaches, as gigabytes of data are generated through messaging and sharing. If it pertains to private health records, enterprise IT professionals must prepare for the inevitable visit by a HIPAA compliance auditor looking for log files and security holes. Increasingly, compliance officers are using event log management software to track key moments where data enters or exits an enterprise, like email systems or the addition or departure of employees with access to sensitive financial data.

What are the penalties for noncompliance?

The consequences for noncompliance with HIPAA regulations can be substantial. The severity of the penalty varies with the infraction; both civil and criminal charges may be levied by the Office for Civil Rights (OCR). The criminal penalties for violating the HIPAA privacy standards can be found in 42 USC 1320d-6 (HIPAA Sec. 1177).

It states that:

> A person who knowingly and in violation of this part:
>
> 1. uses or causes to be used a unique health identifier;
> 2. obtains individually identifiable health information relating to an individual; or
> 3. discloses individually identifiable health information to another person,
>
> Shall be punished as provided below:
>
> 1. be fined not more than $50,000, imprisoned not more than 1 year, or both;

2. if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
3. if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

When it comes to IT operations, compliance with HIPAA has historically been accomplished as part of more generalized security preparations. Healthcare entities generally received attention only when an individual or organization made a complaint. As Kate Norton wrote for SearchSecurity.com in 2007:

Enforcement of the HIPAA Administrative Simplification rules is complaint-driven only -- and at least for the foreseeable future. Privacy rule complaints go to the U.S. Department's Health and Human Services' (HHS) Office for Civil Rights. The OCR handles civil penalties and refers potential criminal complaints to the Department of Justice. All other rules under Administrative Simplification, including the security rule, will be enforced by HHS' Centers for Medicare and Medicaid Services (CMS) Office of HIPAA Standards. This

is true of all "covered entities" large and small. There is no government agency or other body that officially audits proactively for HIPAA compliance.

In 2009, however, HIPAA privacy regulations have teeth. As Randy Nash points out in a recent tip for SearchSecurity.com, the HHS has levied the first penalties against a healthcare agency.

Next article

In this guide

What is the impact of the HITECH Act on IT operations?

http://searchcompliance.techtarget.com/feature/HITECH-FAQ-What-is-the-impact-of-the-HITECH-Act-on-IT-operations

On Feb. 18, 2009, President Barack Obama signed into the law the American Recovery and Reinvestment Act (ARRA) of 2009, commonly known as the "stimulus package." In doing so, President Obama also made the Health Information Technology for Economic and Clinical Health (HITECH) Act the law of the land, in the process significantly expanding the reach of the Health Insurance Portability and Accountability Act (HIPAA) and its corresponding penalties.

This resource provides answers and resources to frequently asked questions regarding the HITECH Act. As you read the FAQ, you'll learn more about what the act is, where it came from, what it requires and what the role of IT is in achieving and maintaining HITECH compliance.

In this guide

What is the HITECH Act?

The HITECH Act is a component of ARRA and of healthcare reform in general, a major legislative focus for the federal government in 2009. HITECH builds on the 1996 Health Insurance Portability and Accountability Act to strengthen the rules designed to protect the privacy and security of health-related data.

The HITECH Act is meant to encourage doctors, hospitals and others in the healthcare industry to make better use of health information technology, allotting some $19 billion in funding for HIT. The HITECH Act created a number of financial incentives for implementing IT infrastructure, including electronic health records (EHRs) technology and training.

The stated purpose behind boosting the use of IT in healthcare is to revamp the way care is delivered, making it more efficient and less prone to error. The initiative will also result in the compilation of vast amounts of data that could be used for research and performance measurement, among other things. The creation of millions of EHRs also makes cybersecurity a critical national priority.

In this guide

The HITECH Act outlines two main goals:

1. Make electronic health records interoperable by establishing standards.
2. Develop a national network for providers to share electronic data.

The act relies on a combination of carrots and sticks to promote those efforts. Financial incentives include grant programs to help pay for IT infrastructure, electronic health records technology and training. A separate set of grants is available to states to give low-interest loans to healthcare providers. A Medicare incentive payment program encourages physicians to be early adopters of electronic health records if they can demonstrate "reasonable use."

At the same time, the act also establishes new privacy and security obligations for anyone covered under HIPAA and extends them to individuals and groups that were not previously covered. The healthcare industry's IT operations now face considerably higher compliance responsibilities as well as greater penalties for noncompliance.

In this guide

How does HITECH extend or augment HIPAA?

HITECH strengthens the rules established under HIPAA for protecting the privacy and security of health information. Enhanced security provisions include a new data breach reporting requirement, which lowers the threshold at which victims must be notified. There are also new disclosure accounting rules, limits on how protected health information can be used for marketing and fundraising purposes and a ban on selling protected data.

HITECH also raises the penalties for noncompliance with HIPAA and provides greater resources for enforcing the rules. It significantly changes the landscape in terms of extending the reach of HIPAA to other entities (see "Who or what is affected by HITECH?").

Who or what is affected by HITECH?

One of the most significant amendments to HIPAA by the HITECH Act is the expansion of the categories of entities subject to the 1996 law's privacy and security rules. Plans and health care clearinghouses are also affected by HITECH, along with their business associates and certain vendors of HIT. All

of the above are now subject to numerous security requirements, including technical, physical and policy-related rules.

The HITECH Act also affects federal healthcare contractors and federal agencies that use healthcare IT systems to exchange health data.

What is generally required by HITECH?

Every entity covered under the HITECH Act has to review its information systems and infrastructure to ensure compliance with the law. These requirements are both extensive and complex, but they can be summarized broadly under two main categories: security and privacy.

HITECH broadens the definition of protected health information. Each entity affected by the law must make sure that it has identified and secured all of the relevant data. Securing this information with technology that matches the U.S. Department of Health and Human Service's (HHS) definition of the "most effective and appropriate technical safeguards" may allow some entities to avoid HITECH's stringent notification requirements in the event of a breach.

In this guide

On Aug. 24, a Final Rule was published in the Federal Register. This guidance further clarified the liabilities for breaches of patients' unsecuredpersonal health information (PHI) incurred by covered entities and business associates liabilities.

Specifically, covered entities must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach. Furthermore:

- If a breach occurs and the data was unsecured, victims must be specifically notified by first-class mail within 60 days of discovery of the breach.
- Covered entities must also notify the media in the event of any data breach of unsecured PHI that involves more than 500 residents of a given state or jurisdiction.
- If more than 500 individuals living in the state are involved, there are additional notification requirements.

A business associate must notify the covered entity of any breach of unsecured PHI, as well as:

1. If the PHI has been irreversibly destroyed prior to unauthorized access.
2. If the breached entity is using National Institute of Standards and Technology standard encryption.
3. If, based on a risk of harm analysis by HHS, it is determined that the unauthorized access will not result in harm.

That last standard from HHS has proven controversial because of the amount of subjectivity involved on the part of the breached entity. The Federal Trade Commission, however, has adopted a more conservative standard for healthcare privacy when it comes to data breach notifications.

Individuals or groups covered under the HITECH Act need to have systems in place for detecting data breaches, recording security incidents and notifying victims as required. All business associate contracts must be amended to include the new requirements to address HITECH compliance.

In this guide

What is the role of IT in HITECH compliance?

Privacy officers, chief information security officers, chief information officers, human resources, customer service departments and operations departments are likely included in any effective compliance program. In fact, part of HITECH compliance is to provide training and ongoing awareness about breach notice procedures to key stakeholders who are outside of IT.

That said, operationally ensuring compliance with HITECH's security and privacy provisions is, to a large degree, an IT function. The security rules established under HIPAA do not require any particular IT system or set of safeguards. HITECH does not impose specific mandates on private entities, either. The HITECH Act does, however, direct HHS to issue guidelines every year on the "most effective and appropriate technical safeguards" for carrying out HIPAA security standards.

Although determination by HHS of what is most effective and appropriate is not a mandate, implementing it can prove beneficial in the event of a breach of protected health information. The HHS guidelines regarding encryption demonstrate one example why: The HITECH Act does not require encryption.

In this guide

HITECH also broadens the category of health information that must be protected. The act directs HHS to define the "minimum necessary" information that data holders must limit themselves to when using, disclosing or requesting protected health information. Until HHS finalizes this definition, information has to be restricted to the limited data set defined in HIPAA privacy regulations. A "limited data set" omits names, street addresses, phone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers and nine other data fields. IT systems involved in the use, disclosure or request of protected data must take into account these restrictions.

HITECH's privacy requirements also include restrictions on the use of protected health information for marketing and fundraising purposes, a prohibition on selling information, a mandate to agree to requests for restricting the use and disclosure of data, and rules on accounting for the disclosure of data. HITECH compliance, given these requirements, will likely have an impact on the kinds of IT systems and infrastructure deployed.

What are the penalties for noncompliance?

The HITECH Act increases the civil monetary penalties for HIPAA noncompliance to as much as $50,000 per violation. The violator's level of intent is taken into account, however -- if he can prove he did not know about a violation, the penalty could be as little as $100 per violation. Violations resulting from "reasonable cause" but not "willful neglect" start at $1,000. Violations of "willful neglect" can result in penalties of $10,000 per violation. Under each of these tiers, there is a cap on the total penalty that can be imposed for the same type of violation in a given year.

In addition to heightened monetary penalties, HITECH authorizes state attorneys general to enforce HIPAA privacy and security requirements under certain circumstances. The act also authorizes HHS to conduct audits to ensure compliance with both HITECH's provisions and HIPAA's privacy and security requirements.

There are criminal penalty provisions under HIPAA as well. According to Rebecca Herold's SearchCompliance.com article on HIPAA enforcement, the regulation originally "provided for criminal penalties of fines of up to

$250,000 and up to 10 years in prison for disclosing or obtaining PHI with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm." HITECH extends these provisions to the business associates of anyone covered under HIPAA.

As Herold points out, more government audits are also leading to more convictions. "The HITECH Act also permits the Office for Civil Rights (OCR) to pursue an investigation and apply civil monetary penalties against individuals for criminal violations of the HIPAA Privacy Rule and Security Rule if the Justice Department did not prosecute the individuals," she writes. "Additionally, the HITECH Act changes HIPAA to require formal investigations of complaints and to impose civil monetary penalties for violations resulting from willful neglect. Any civil monetary penalties collected must then be transferred to OCR to use for HIPAA enforcement activities, and the HHS must establish a process to distribute a percentage of the collected HIPAA penalties to harmed individuals."

In this guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers—a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia