TechTarget

E-Guide

HIPAA Omnibus Compliance Guide

A compilation of our best educational content from editors and experts to prepare you for HIPAA omnibus rule, coming in effect September 2013

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Dear Health IT Professional,

The package of information you just downloaded was written and assembled as a guide for health IT professionals, like yourself, interested in content and compliance information on HIPAA omnibus – which goes into effect September 2013.

Given the positive response and feedback we've received from our HIPAA-related content – SearchHealthIT.com's team of editors decided to extend this information and make it available to a wider audience. As a result, we have complied all relevant HIPAA omnibus content in one, easy-to-access e-guide for your convenience. Included in this report, you will find featured articles on:

- 10 grains of wisdom from the final HIPAA omnibus rule
- How the changes affect IT security pros
- New breach notification rules demanding documentation
- HIPAA omnibus and stage 2 testing organizational compliance
- And much more!

We hope you enjoy this package of information and find it useful when developing your new compliance plan.

Don't forget to visit SearchHealthIT.com to get the latest information and news from our award winning editorial staff and industry experts – we'll be releasing additional articles and tips that will keep you informed and prepared as we approach the September deadline.

Best Regards,

SearchHealthIT.com

P.S. Don't forget to join our online community and be the first to hear breaking news and event announcements! **Follow us on Twitter @SearchHealthIT**

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

About SearchHealthIT.com

SearchHealthIT.com is the health care technology professional's guide to building and managing an electronic health care infrastructure. SearchHealthIT.com provides free unbiased news, analysis, resources and strategies for health care IT professionals that manage health care operations for hospitals, medical centers, health care networks and other providers.

We know that patient care at your organization is your number one concern. That's why we are dedicated to providing you with the tools, guides and techniques to improve efficiencies, cut costs, and meet regulatory requirements.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule ..... *Page 3*

New breach notification rules demand documentation ..... *Page 5*

HIPAA omnibus rule: Compliance tips for provider preparedness ..... *Page 7*

The HIPAA omnibus rule: How the changes affect IT security pros ..... *Page 8*

HIPAA regulations to bring compliance challenges for providers, BAs ..... *Page 11*

Tip: HIPAA omnibus rule and stage 2 test organizational compliance ..... *Page 13*

Quiz: HIPAA omnibus rule ..... *Page 17*

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Ten more grains of wisdom from the final HIPAA omnibus rule

Don Fluckinger, *News Director, SearchHealthIT.com*

Health care providers and other covered entities and business associates can begin poring over the HIPAA omnibus rule, released Jan. 17 by the U.S. Department of Health & Human Services' Office for Civil Rights. The 563-page rule outlines OCR's data privacy and security enforcement strategies, which have been updated for the EHR era as mandated by the HITECH Act.

The proposed rule was released in July 2010, and the final rule was at the Office of Management and Budget (OMB) since March 2012, a stop that usually amounts to a few weeks before U.S. government agencies publish regulations in the Federal Register. But officials delayed the final release, as they sought to address stakeholder concerns regarding data breach thresholds and enforcement policies. In June, National HIT Coordinator Farzad Mostashari, M.D., predicted the Health Insurance Portability and Accountability (HIPAA) omnibus rule would be out by the end of the summer. Now it's here, and the enforcement clock begins ticking. The omnibus rule goes into effect March 26, and covered entities have 180 days -- or until Sept. 22, 2013 -- to get into compliance. Here are 10 other pieces of information from the final rule for covered entities and their business associates to be aware of:

1. According to a regulatory impact analysis contained in the rule, the Office of Civil Rights (OCR) estimates between 200,000 and 500,000 business associates of some 19,000 covered entities exist in the country. The American Hospital Association estimates there are not quite 6,000 registered U.S. hospitals.
2. OCR sides with consumer advocates, who wanted to be sure all "electronic designated record sets" are available to patients. This decision goes against other industry stakeholders, who wanted to limit that requirement to access to electronic health records (EHRs).
3. When a covered entity requires patients make a "written" request for their records, patients may now request their records electronically --

and sign those requests electronically -- if the organization chooses to support the technology.

4. If a patient wants their data to be placed on an external media drive, like a thumb drive, providers are not mandated to accept the device if their organization has conducted a HIPAA risk analysis and found external drives to be a risk. However, if they reject a patient's thumb drive, they can't require the patient to purchase one the covered entity provides. Instead, they have to find an alternative distribution method, such as email.
5. The OCR did not define EHRs, but clarified that patients do have access to electronic copies of their health information wherever the data is housed.
6. Covered entities are not liable for unauthorized access to unencrypted emails if patients want to receive their data that way. OCR said in the rule: "We do not expect covered entities to educate individuals about encryption technology and information security. If individuals are notified of the risks, and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request [or once it's delivered]."
7. A provider can wait 30 days between a patient's request for data and delivering it, with a 30-day extension when necessary. But OCR hopes organizations don't wait that long. "We encourage covered entities to provide individuals with access to their information sooner, and to take advantage of technologies that provide individuals with immediate access to their health information."
8. Patient safety organizations, health information organizations (HIOs), e-prescribing gateways and "other persons that facilitate data transmission", as well as personal health records vendors, are explicitly named as business associates. OCR chose the term "HIO" because it includes both health information exchanges and regional health information organizations.
9. Subcontractors of business associates are now the same category as business associates, in the compliance sense.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

10. Many factors will go into determining the size of fines. Three of them are: whether the covered entity or business associate had financial difficulties that affected compliance; whether the imposition of a civil money penalty would jeopardize the ability of the organization to continue to provide or pay for health care; and..."such other matters as justice may require."■

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

New breach notification rules demand documentation

Ed Burns, *News Writer, SearchHealthIT.com*

After a wait of nearly three years, the U.S. Department of Health and Human Service's Office for Civil Rights released the much-anticipated update to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, also known as the HIPAA omnibus. Read the reactions from industry experts in this two-part feature.

Another major development out of the HIPAA omnibus is the premium that Office for Civil Rights (OCR) officials place on documenting privacy and security policies, as well as responses to breaches. In particular, the changes to the breach notification rule set the bar high for documentation, and covered entities that fail to keep adequate records could face enforcement actions, even when their general response to a breach is appropriate.

The interim rule used a harm threshold to assess whether a covered entity was subject to penalties in the event of a data breach. This criterion forced providers to assess whether a breach was likely to result in significant financial, reputational or other harm to patients. The updated rule eliminates the threshold and assumes harm anytime there is a high probability that personal health information (PHI) has been compromised. It is up to the covered entity to assess whether an event such as a lost thumb drive or network intrusion is likely to have compromised PHI and to report any such cases to the OCR.

Doug Pollack, chief marketing officer at ID Experts, said this is a much more objective standard that will likely lead to more breach reporting. But organizations shouldn't worry they will be fined every time they report a

breach. Those who have clearly documented their security policies and their method of responding to the breach are less likely to be fined, he said.

But many health organizations will have to change their culture to ensure this kind of documentation takes place. Health care organizations often don't make security a top priority, and compliance efforts tend to be underfunded, said Carlos Leyva, attorney and managing partner at the Digital Business Law Group of Pennsylvania. To comply with the new rules providers are going to have to examine how they approach security and privacy. The changes should start at the top.

"Until you reach the executive suite and they get it, not much is going to change," Leyva said. "That poor compliance officer just has that title, they don't have the budget. This is an executive-suite issue."

Leyva said an organization could do everything right when it comes to protecting PHI and responding to breaches. But if it doesn't have these policies and procedures documented appropriately, they become nothing more than "empty promises" during an OCR investigation. In this case the enforcement agency will assume the organization's procedures were inadequate and likely take action against the provider.

Because of the enhanced documentation requirements and other provisions, Lisa Sotto, head of the global privacy and data security practice at the law firm Hunton and Williams, sees the omnibus rules as creating major new burdens for providers, some of which she described as "administrative nightmares." The elimination of the harm threshold will force organizations to investigate any possible misuse of PHI and document the entire process. This could result in providers spending significant time reviewing small events.

"Breaches happen all the time," Sotto said. "They are ubiquitous. Most of them are absolutely harmless and innocuous, but others are less innocuous. It adds enormous burdens." ■

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

HIPAA omnibus rule: Compliance tips for provider preparedness

Don Fluckinger, *News Director, SearchHealthIT.com*

The HIPAA omnibus rule is here; set to go into effect Sept. 23. Attorney Adam Greene -- former federal HIPAA regulator and current partner at Davis Wright Tremaine LLP -- broke down some of the key areas of the law for health care providers to consider while updating their compliance plans.

"The wait is over … there are no more excuses for not jumping in and reassessing and approving your HIPAA compliance," Greene said in a webinar sponsored by data breach prevention and response services vendor ID Experts. While it would be impossible to be comprehensive in an hour-long presentation -- the HIPAA omnibus rule is 563 pages, after all -- Greene called attention to some HIPAA hot spots where this updated regulation shines a sharp spotlight and might change current compliance strategies:

- **Business associates and their subcontractors are now, in effect, covered entities.** That means they are subject to random HIPAA compliance audits, too.
- **There are likely more business associates in your universe.** Before, if you used or disclosed protected health information (PHI) on behalf of a covered entity, you were a business associate. That definition expands to now include any party who "creates, receives, maintains or transmits PHI" for a covered entity.
- **Rework those business associate contracts** to include verbiage acknowledging they understand they now must comply with breach notification rules. In some cases, CMS grants a one-year grandfather period to remake those agreements with a deadline of Sept. 23, 2014.
- **Immunization records can be released to schools without authorization.** Read the fine print here, too -- there are caveats.
- **PHI isn't PHI 50 years after a patient's death.** Furthermore, a covered entity may disclose PHI to persons involved in the decedent's care or payment -- if that doesn't run contrary to the patient's prior expressed preference.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

- **More rules around genetic information.** First, genetic data is now health information. Second, a health plan (other than long-term care plans) may not use or disclose genetic information for underwriting purposes.
- **Rules about using PHI for fundraising and marketing have changed, as well as sale of PHI.** Dive into these sections; some rules around fundraising have been loosened -- as long as the covered entity follows HIPAA rules that outline patient opt-out policies. Rules governing marketing with PHI and sale of PHI, however, have been tightened.
- **Non-disclosure of services paid out of pocket:** Here's a data management puzzle for the CIO and HIM manager to solve together -- when patients fully pay out of pocket for care and request their health plans not know about it, the covered entity must comply. Unless, of course, non-disclosure is prohibited by law.
- **There's more to come.** Missing in the HIPAA omnibus rule and yet to be issued by CMS include clarifications on: how covered entities will account for PHI disclosures and create PHI access reports; the "minimum necessary" standards of disclosure of PHI during the course of care; and an outline of what portion of penalties and settlements that the HHS Office of Civil Rights collects will be distributed to patients harmed by a data breach, and how that will happen.■

The HIPAA omnibus rule: How the changes affect IT security pros

Mike Chapple, *Ph.D., CISA, CISSP, IT Security Manager,University of Notre Dame*

The Health Insurance Portability and Accountability Act (HIPAA) has a long history in the world of IT compliance.

From the initial release of the HIPAA Security Rule in 2003 through the passage of the HITECH Act in 2009, information security professionals in the health care industry have focused on implementing controls designed to protect the confidentiality, integrity and availability of electronic protected

health information (ePHI). The Department of Health and Human Services' (HHS) January 2013 release of the HIPAA Omnibus Rule opens the next chapter in HIPAA compliance initiatives.

The new omnibus rule technically went into effect in late March, but organizations subject to HIPAA have until Sept. 23, 2013, to become fully compliant with the new regulation. For security practitioners, there are two particular points of interest: the rule's new view on data breaches and the expansion of HIPAA's provisions to include business associates. In this tip, we look at these two changes and their impact on IT security professionals who support enterprise compliance efforts.

Data breaches and the risk of harm standard

During the rulemaking process that led to the HIPAA Omnibus Rule, there was quite a bit of debate between the health care and privacy communities regarding how the regulation would define a data breach. This is important because it spells out exactly when a breach or loss of data must be reported to individuals, the media and/or HHS, exposing an organization to reputational damage and possible fines. Privacy advocates argued that any potential disclosure of personal information should be considered a data breach, while opponents countered that HHS should follow the more complex "risk of harm" definition in the draft regulation. If adopted, this standard would have required that for an incident to be defined as a breach, it must be shown to cause "a significant risk of financial, reputational or other harm to an individual."

A compromise was reached so that under the new Omnibus Rule definition, breach notification is required when a covered entity or business associate experiences an impermissible use or disclosure of protected health information (PHI). If these circumstances arise, an event is presumed to be a breach unless the *entity* can prove that there is a low probability that the PHI has been compromised. This creates a presumption that a breach occurred that the covered entity must overcome.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Organizations subject to the provisions of HIPAA should take the opportunity to reevaluate their existing incident response and breach notification practices to ensure that they are in compliance with the new mandate. This should include verifying the consistency in definitions between HIPAA's requirement and the organization's practice, and the risk assessment necessary to determine whether an incident is considered a breach. Additionally, policies and procedures that implement the requirements to notify both HHS and affected individuals when a breach occurs should be in place.

Extending HIPAA's reach to business associates

The Omnibus Rule also creates new responsibilities for the business associates of HIPAA covered entities who handle protected health information. While the original HIPAA rules required covered entities to enter into business associate agreements (BAAs) with their partners, the new rules extend the authority of HHS to regulate those business associates, as well as any subcontractors they employ.

From a compliance perspective, covered entities should review all of their business practices to ensure they have correctly identified business associates, and then review the BAAs they have in place to ensure that they require organizations to comply with the HIPAA Privacy Rule and Security Rule. Organizations that serve as business associates should conduct gap and risk assessments to ensure that they comply with the rules and understand their legal responsibilities to both the covered entity and HHS. Expect to see enforcement actions from HHS against business associates later this year, after the Sept. 23, 2013, compliance deadline passes.

Conclusion

Overall, security practitioners will not be tremendously affected by the new Omnibus Rule. While other provisions of the rule do have some significant potential business effects, such as providing patients with the right to receive electronic copies of their medical records and requiring authorization and opt-out capabilities for certain marketing and fundraising activities, the security

implications should be manageable. Covered entities that appropriately tweak their incident response and business associate practices should find themselves with little to change, from a security perspective.■

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

HIPAA regulations to bring compliance challenges for providers, BAs

Ed Burns, *News Writer, SearchHealthIT.com*

Providers have about six months to comply with the changes to privacy and security practices mandated by the HIPAA omnibus rule. The new rules could give some organizations headaches, and not just because they represent technical challenges.

Speaking at the HealthTech Council meeting in Chicago, Kirk Nahra, partner at the law firm Wiley Rein LLP, said the new privacy and security regulations will force providers to make significant changes to some of their processes, but often without much actual benefit to the patient.

Nahra discussed, for example, how the new breach notification rules mirror those of other industries -- banking, for instance. However, when a person's financial records are lost or stolen, notifying customers is important because there are concrete steps they can take to protect themselves from further damage. They can close out accounts or monitor their credit reports more closely. The situation is not so clear in healthcare, Nahra said: There isn't much patients can do to protect themselves from further harm by learning of an inappropriate disclosure of their diagnoses or medications.

The new rules give patients the right to receive an accounting of every employee at their provider who touched their protected health information (PHI). Nahra called this one of the biggest wastes of time in the HIPAA regulations, because it will require hospitals to keep exhaustive records for a right that few patients are aware they have or will take advantage of. Even though the U.S. Department of Health and Human Services (HHS) made the rule with an eye toward patient empowerment, an appropriate goal, the specifics could put providers in a difficult position, he said. "Think about all the record-keeping that would be required of that," he added. "HHS is feeling

its way on what it wants to do for patients. The rationale for this was patient empowerment. I don't think they've given up on getting patients more involved in their care."

Furthermore, Nahra said, he doesn't think the HIPAA regulations do as much to protect patients' information as most providers, patients or lawmakers believe. "HIPAA is not a healthcare privacy law," he said. "It protects certain kinds of health information when it's held by certain professionals in certain situations."

For example, when patients submit a medical record to their health insurance company after a car accident, the information is subject to HIPAA privacy regulations, but when those patients submit the exact same record to their car insurance company, the information is not subject to any privacy laws.

Linda Koontz, senior principal at Mitre Corp., said most of the updated HIPAA regulations reflect the desire of HHS to protect patients' health information regardless of where it goes throughout the healthcare system. A third-party data storage company should be held accountable for losing health data, just as providers are. But, she acknowledged, many of the new rules will be difficult to comply with, particularly for business associates, who now are liable for breaches just like covered entities under the new rules. Some might not even be aware of their new responsibilities.

Possibly the biggest change made by the HIPAA omnibus rule is the standard used to judge breaches. Koontz explained that regulators previously used a harm threshold test in the case of a data breach to determine whether penalties applied and patients had to be notified. But when the new rule goes into effect, it presumes harm in all breaches. Providers will have to prove that the disclosure of information is unlikely to lead to real harm to patients.

Nahra recommended that in order to prepare for this change, providers evaluate their next breach under both criteria. He believes that the outcome will be mostly the same under both tests, but it will be a helpful exercise. This

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

might seem like a burdensome extra step now, but it could help hospitals get ready for the privacy and security changes coming their way. ■

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Michael Frederick, *President and CEO of The Frederick Group*

The words "meaningful" and "use" are undoubtedly on the lips of many a CIO as 2014 approaches and brings with it stage 2 of the federal EHR incentive programs, and especially in light of the recent omnibus HIPAA privacy and security rule. Final requirements outlining criteria for the certification of EHR technology for stage 2 meaningful use were published in September 2012. Meaningful use under the stage 1 criteria, which focused on data capturing and sharing in 2011 and 2012, must have been achieved before providers can move on to stage 2.

Among the stage 2 criteria is specific detail about data encryption required for EHR certification. Core measure 7 of the stage 2 eligible hospital and critical access hospital (CAH) measures outlines several key areas:

- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in [certified EHR technology] CEHRT in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3).
- Eligible hospitals and CAHs must conduct or review a security risk analysis of [CEHRT], including addressing encryption/security of data, and implement updates as necessary at least once prior to the end of the EHR reporting period and attest to that conduct or review.
- Eligible hospitals and CAHs are not required to report to CMS or the states on specific data encryption methods used. However, they are required to address the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312(a) (2)(iv) and 45 CFR 164.306(d)(3).

Other stage 2 encryption requirements include:

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

- Protecting patient health information with at least a symmetric, 128-bit fixed-block cipher algorithm capable of using a 128-, 192-, or 256-bit encryption key when furnishing electronic copies of patient health information.
- Developing a username for each user.
- Encrypting and decrypting health information when using removable media.

Changes on the horizon: Omnibus HIPAA rule

On Jan. 17, 2013, the Department of Health and Human Services' Office for Civil Rights announced the new omnibus HIPAA rule intended to "improve privacy protections and security safeguards for consumer health data."

Four final rules covering a wide range of HIPAA-related issues are included in the omnibus rule, chief among them being the increased compliance responsibility placed on business associates in protecting health information and reporting breaches. Previously, the rules focused on health care providers and health plans.

The OCR's "significant harm" standard, in place since the interim final breach notification rule was released in 2009, has been replaced with a "low probability" standard. This puts the onus on covered entities and business associates to conduct formal risk assessments for breach notifications even if they don't believe the breach is significant. Penalties for noncompliance will be assessed within a tiered structure based on the extent of negligence, and can reach a maximum of $1.5 million per violation.

The HIPAA rule could mean significant changes to the way contractors and subcontractors treat data encryption. EHR vendors only have to be able to show that they encrypt the data that is stored on an endpoint device, or show that they don't allow the saving of information to a device. However, the increased responsibility placed on business associates includes contractors and subcontractors.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

All about incentives

Under the HITECH Act, incentive payments are available to eligible health care professionals and hospitals that adopt certified EHR technology and demonstrate meaningful use of certified technology. In effect, these are reimbursement payments to help defray -- or even cover in their entirety -- providers' upfront costs to meet EHR certification requirements.

It must be noted that providers are eligible for reimbursement *only* if they use certified EHR systems.

Supporting EHR encryption

CIOs will take different methods to achieve EHR compliance depending on the size of the organization; the age of the existing system **to be updated, upgraded, or replaced outright;** and, of course, whether the objective is qualifying for incentives.

When it comes to data encryption alone, there are a number of questions CIOs need to consider:

- Can simple software updates be made to an existing system, or is it necessary to start from scratch?
- Is patient data currently encrypted, and if so, does encryption extend to backup storage and removable media?
- What would be involved in a data migration strategy?
- Is current data being stored on on-site servers, and if so, is it time to consider cloud-based storage?
- Is there an IT security resource that is already qualified to do the work, or is it necessary to research new resources?
- Can a new resource be leveraged for budget purposes and integrated with other products?
- What is the cost involved in ongoing IT and/or training support after implementation?

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

The first step in figuring out how to proceed is to perform an audit of your current system and processes in combination with a risk analysis. Once you have identified your objectives in the context of your current circumstances, it's time to consider how to move forward.

But always remember this: The goal is not just EHR certification and compliance. It is mitigated risk in a continually volatile environment, especially given the new tiered breach-violation figures. Just consider a few recent HIPAA breaches:

- Emory Healthcare in Atlanta misplaced 10 backup disks containing information for more than 315,000 patients. Costs are expected to climb beyond $3 million.
- California's Sutter Health had a computer stolen that contained confidential information on 4.2 million patients. A class action lawsuit was filed in late 2011 for $1 billion.
- Tricare's data breach in 2011 affected 4.9 million patients from the past 20 years. Unencrypted backup tapes were stolen while in transit from one work site to another. In addition to fines, a class action lawsuit is asking $1,000 per patient, for a total of $4.9 billion.

The Office of the National Coordinator for Health Information Technology (ONC) lists products certified for meaningful use. Per the ONC, each complete EHR and EHR module listed on the website has been tested and certified by an ONC-Authorized Testing and Certification Body.

Preparing for EHR stage 2 and beyond

By most accounts, implementing stage 1 requirements and preparing for stage 2 is no easy undertaking, even considering just the time involved and manpower required. Add in the expense of new systems, the implementation of new security measures, and the training that will be needed for new compliance protocols, and expenses increase.

As expenses increase, so does anxiety. However, the Medicare and Medicaid incentives that offset upfront costs help, as does the enhanced

security that can help lower the probability of HIPAA breaches. Success is as much in mitigating the opportunities for failure as it is implementing new systems.

Preparation and continuity are keys to successful EHR integration, which begins with analyzing what needs to be changed but doesn't end at implementation.

Here are some tips for succeeding with EHRs:

- Do a gap analysis. Looking at where you are now versus where you need to be can provide a clear path.
- Identify and prioritize implementations.
- Research. You'll know the solution that works best for you only by examining all the possibilities.
- Consider the upsides of an upfront spend. No one wants to pay fines and be faced with a lawsuit because a backup disk or laptop was compromised.
- Train the workforce on new security measures. Your security is only as good as your least-informed team member.
- Establish policies and procedures in concert with compliance.
- Test and retest compliance procedures and readiness, and tinker where necessary.
- Investigate customization opportunities that further prepare your team for ongoing compliance.

Making your compliance team part of the solution means they won't part of the problem. Consult them early and often.■

Quiz: HIPAA omnibus rule

Test your knowledge of the HIPAA Omnibus rule. Use this five-question quiz to reinforce your understanding of the key concepts related to rule. Arm yourself and your organization with the information needed to be in compliance this September.

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Quiz Questions:

1. Which of these facts about the HIPAA omnibus rule is false?
2. Which groups are not considered covered entities under the HIPAA omnibus rule?
3. Which aspects of the HIPAA omnibus rule have been dubbed potential burdens by industry experts?
4. Which is not a noteworthy update for professionals adjusting their compliance plans?
5. How will the HIPAA omnibus rule affect data breaches?

Click here to access this quiz online

Answer Key:

1. C – The Office of the National Coordinator for Health Information Technology (ONC) released the rule
2. A – The U.S. Postal Service, United Parcel Service, delivery truck line operators and certain Internet service providers
3. E – All of the above
4. D – The included outline of what portion of penalties and settlements the HHS Office of Civil Rights collects will be distributed to patients harmed by a data breach
5. D – Health organizations will have to start at the top to change their culture and ensure that they clearly document their security policies and methods for responding to breaches

Contents

Ten more grains of wisdom from the final HIPAA omnibus rule

New breach notification rules demand documentation

HIPAA omnibus rule: Compliance tips for provider preparedness

The HIPAA omnibus rule: How the changes affect IT security pros

HIPAA regulations to bring compliance challenges for providers, BAs

Tip: HIPAA omnibus rule and stage 2 test organizational compliance

Quiz: HIPAA omnibus rule

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

SearchHealthIT

Health IT Exchange