866-726-4271
info@idexpertscorp.com

WHITEPAPER

The HIPAA Final Omnibus Rule

An analysis of the changes impacting healthcare covered entities and business associates

According to the Third Annual Benchmark Study on Patient Privacy & Data Security by Ponemon Institute,[1] 94 percent of healthcare organizations suffered data breaches, costing the healthcare industry an average of $7 billion a year. Data breaches risk the medical and financial well being of breach victims and the credibility and future business of healthcare providers.

At the same time, federal and state governments are issuing even more regulations in response to the growing public concern and eroding public trust over the PHI breach epidemic. The most sweeping of these regulations is the long-awaited HIPAA Final Omnibus Rule.[2]

Published in the Federal Register on January 25, 2013, by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the HIPAA Final Omnibus Rule is landmark legislation that affects nearly every aspect of patient privacy and data security. It encompasses four rules:

1. Modification of the HIPAA Privacy, Security, and Enforcement Rules to include HITECH requirements
2. Modification of the Breach Notification Rule
3. Modification of the HIPAA Privacy Rule regarding the Genetic Information Discrimination Act of 2008
4. Additional modifications to the HIPAA Rules

The HIPAA Final Omnibus Rule aims to increase patient privacy protections and provide greater control of their personal health information while strengthening OCR's ability to enforce the law. While many aspects of the rules were upheld, there are significant changes that must be addressed. With the Final Rule to take effect on September 23, 2013, healthcare organizations — covered entities and their business associates — need to act now to implement compliance systems and processes.

Privacy and security professionals at ID Experts analyzed the Final Rule to provide insights that help covered entities and their business associates understand the new law and how it affects their polices and procedures, security measures, and daily interactions with patients. This paper provides those insights as well as steps entities can take now to help achieve compliance.

A Brief History of HIPAA and the Changes Through the Years

To help protect against the breach of personal medical information, the Health Insurance Portability and Accountability Act (HIPAA),

1. Third Annual Benchmark Study on Patient Privacy & Data Security by Ponemon Institute, December 2012. See www2.idexpertscorp.com/ponemon2012
2. Text of the Final Rule can be found at: www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

enacted in 1996, set standards for medical privacy that went into effect over the next 10 years. The American Recovery and Reinvestment Act (ARRA), signed by President Obama in February 2009, put into law new privacy requirements that experts at the time called "the biggest change to the healthcare privacy and security environment since the original HIPAA privacy rule."[3]

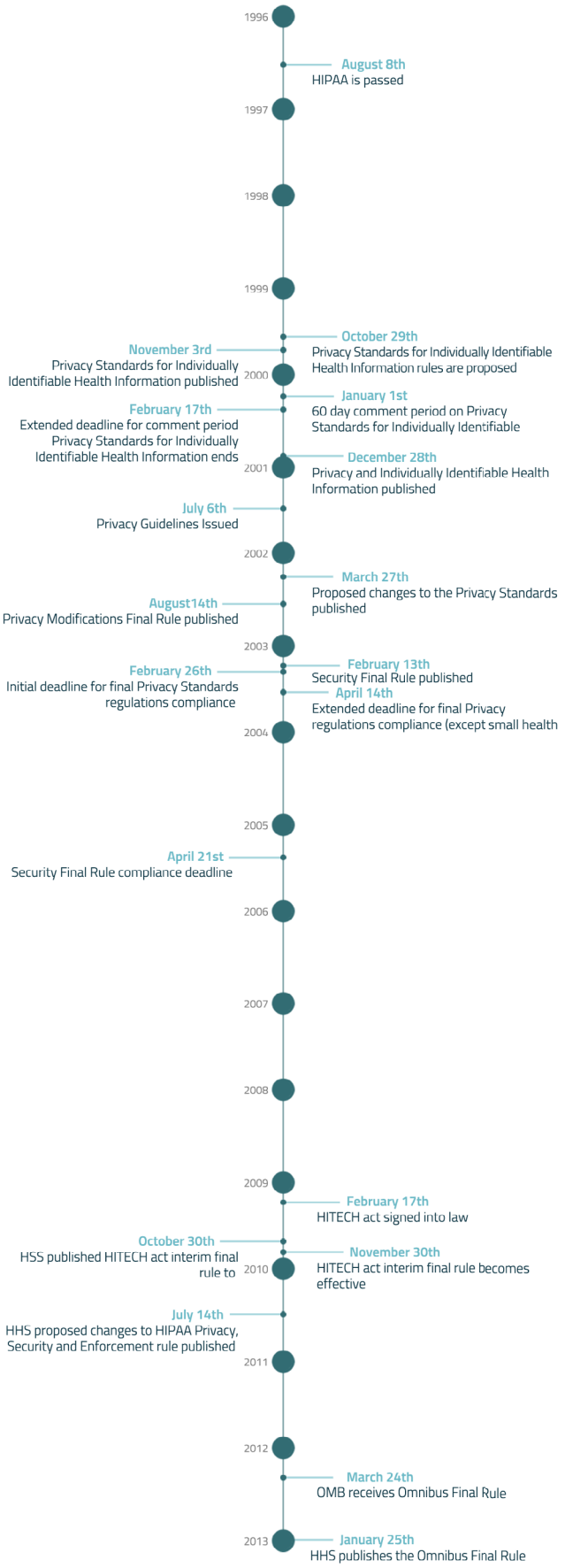
Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, sought to streamline healthcare and reduce costs through the use of health information technology. The HITECH Act dedicated over $31 billion in stimulus funds for healthcare infrastructure and the adoption of electronic health records (EHR), including funding for the meaningful use incentive programs. To ensure that privacy and data security went hand in hand with the digitization of health records, healthcare organizations had to comply with the HIPAA Privacy and Security Rules by establishing a risk management process and conducting annual risk assessments.

The HITECH Act also imposed new requirements, including:

- Specific thresholds, response timeline, and methods for breach victim notification.
- A new definition of business associates and extension of the HIPAA privacy and security requirements to include business associates.
- Expansion of contractual obligation for security and privacy of PHI to subcontractors of business associates.
- Tiered increase in penalties for violations of these rules, some of them mandatory, with potential fines ranging from $25,000 to as much as $1.5 million, effective immediately.
- Provisions for more aggressive enforcement by the federal government.
- Explicit authority for state Attorneys General to enforce HIPAA Rules and to pursue HIPAA criminal and civil cases against HIPAA covered entities (CEs), employees of CEs, or their business associates.
- Requirement for the Department of Health and Human Services (HHS) to conduct mandatory audits.

The HITECH Act allowed only one year for most provisions to be enforced. On September 23, 2009, the Department of Health and Human Services issued guidelines on the HITECH Act, known as the Interim Final Rule for Breach Notification. This rule, among other things, included a controversial "harm threshold" that gave CEs the responsibility for determining whether notification is required after discovery of a breach of PHI. The HHS submitted a final rule for review to the Office of Budget and Management, only to withdraw it in July 2010. Now, more than two and a half years later, the HIPAA Final Omnibus Rule is finally here.

The Story So Far
A HIPAA/HITCH Timeline



3 Kirk J. Nahra, Wiley Rein LLP, and Rick Kam and Mahmood Sher-Jan, ID Experts. "Ready for Data Breaches Under the HITECH Act?" Webinar. May 27, 2010.

The Edicts and the Impacts: Why You Need to Know and Care

The HIPAA Final Omnibus Rule includes significant modifications to certain portions of the rules, while others were adopted with little or no change. In either case, these requirements affect every aspect of your operations, and compliance could entail considerable resources and cost. It is critical to understand these requirements — changed or not — and their impact so you can protect your organization while minimizing expenses.

Breach Notification

Under the interim final rule, a breach crossed the harm threshold if it "pose[d] a significant risk of financial, reputational, or other harm to the individual." Opponents claimed that placing the burden of proof for determining this risk of harm on covered entities caused huge (subjective) variances in the definition of a notifiable breach, leaving affected individuals at risk for harm. They also claimed it burdened HHS to judge if the assessments met the intent of the rule.

The HIPAA Final Omnibus Rule seeks to better protect patients by removing the harm standard and replacing it with a new compromise standard. However, the Final Rule does not explicitly define the term "compromise." Covered entities and their business associates must still conduct an incident risk assessment for every data security incident that involves PHI. Rather than determine the risk of harm, however, the risk assessment determines the probability that PHI has been compromised.

The compromise standard is based on a minimum four factors that are derived from factors previously listed in the interim final rule:

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

HHS points out that healthcare organizations must consider all these factors together when determining the overall probability that PHI was compromised. If an entity has a security or privacy incident involving PHI, and its risk assessment concludes there was a very low probability that PHI was compromised, it may choose to not notify the affected individuals or the HHS Office for Civil Rights. However, the Final Rule requires that the entity maintain a burden of proof if its conclusions are called into question.

It remains to be seen whether the Final Rule achieves its goal of consistent risk assessment outcomes; the outlined factors still allow consideration of any adverse impact to the affected individual. Additionally, the Final Rule leaves room for entities to claim exception from notification even if the incident does not match the existing exception criteria. However, the interim final rule does strike a better balance by explicitly identifying the risk assessment factors while recognizing the complexity and some subjectivity that is inherent to any risk assessment.

If investigated, a covered entity must provide conclusive documentation of its incident risk assessment and analysis as to why the incident did not result in a compromise of PHI. If the entity doesn't meet that burden of proof, it could be found to have been negligent in not notifying the affected individuals and subject to substantial fines, penalties, and corrective action.

OCR may work with covered entities to achieve voluntary compliance through informal resolution. OCR also has the authority to impose a civil money penalty for violation of the HIPAA Privacy Rule, even in cases where the entity made all required breach notifications.

And the Survey Says . . . Four or More Data Breaches

A new survey by the Health Care Compliance Association and the Society of Corporate Compliance and Ethics[4] indicates that 59 percent of those surveyed had an incident in the past year, while 20 percent of organizations have suf¬fered four or more breaches.

Notification and Other Provisions

With one small exception, the Final Rule upholds the timeline for notification to individuals, HHS, media, and by business associates to covered entities — "without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach." Content and methods of notification remain the same under the Final Rule.

The interim final rule provided an exception for limited data sets that did not contain birth dates or zip codes. The Final Rule removes that exception, requiring healthcare organizations to conduct a risk assessment following every PHI privacy or security incident to determine if notification is required. The Final Rule retains three other exceptions and the encryption safe-harbor from the interim final rule. *(Continued on page 6)*

4. See "Health data breach trends from HCCA, SCCE survey, " January 25, 2013, HealthITSecurity.com

HIPAA Final Omnibus Rule Requirements & Impacts

	Requirement	Impact
Breach Notification	New definition of a breach replaces the "risk of harm" standard with the "probability" that PHI has been compromised. The entity retains the burden of proof, however.	• CEs and BAs must conduct and document an objective risk assessment to determine probability and support their decision to notify or not notify. • Risk assessments must include steps taken to mitigate risks to PHI. • CEs and BAs are still required to "mitigate adverse consequences" and to notify individuals when the probability of PHI being compromised is not low. • Entities must update policies and procedures and retrain their workforce.
	The exception for limited data sets that did not contain birth dates or zip codes has been removed.	• Entities must conduct risk assessments following all PHI privacy or security incidents.
	State and federal laws are more aligned.	• More stringent state laws may be applied, as long as they are not contrary to federal law.
Business Associates	Expanded definition of a business associate is one that creates, receives, maintains, or transmits PHI on behalf of a covered entity, as well as other specific types of organizations.	• "New" business associates have the same liability as existing BAs. • They must bring business processes and systems into compliance with HIPAA Rules. • CEs must enter into appropriate contracts with these new BAs.
	Subcontractors are now considered business associates and are bound by the same HIPAA privacy and security requirements.	• Subcontractors must bring business systems and processes into compliance with HIPAA privacy and security requirements. • BAs must revise contracts with subcontractors to reflect HIPAA requirements.
	Business associate contracts must specify requirements for breach notification, electronic access to PHI, etc.	• BA contracts must specify compliance with the Breach Notification Rule. • If a CE designates HIPAA liability, the contract must specify BA compliance. • Contracts must specify to whom the BA provides electronic access to PHI. • One-year grandfathering may be available.
Increased Enforecement of Willful Neglect	OCR enforcement focuses on willful neglect, defined to be "conscious, intentional failure or reckless indifference."	OCR will: • Investigate all cases of possible willful neglect. • Impose a penalty on all violations of willful neglect.
Patient Rights	Restriction of disclosure for out-of-pocket payments	• CEs must agree to an individual's request to restrict disclosure to a health plan if the individual pays in full for a service or item.
	Copies of PHI to third parties must be authorized.	• Authorization must be made in writing, and clearly identify the recipient and where to send the copy.

	Requirement	Impact
	Electronic copies of PHI must be made available.	• CEs must provide a readable electronic copy of PHI, rather than a hard copy, even if it is not readily producible.
Notice of Privacy Practices	Changes to notice of privacy practices	CEs must change their notice of privacy practices to include: • Prohibition of sale of PHI • Duty to notify in case of a breach • Right to opt out of fundraising • Right to restrict disclosure for out-of-pocket payments • Limit on use of genetic information
Use and Disclosure of PHI	New categories of PHI may be used or disclosed for fundraising.	• Healthcare organizations can better target their fundraising efforts based on these categories.
	Strengthened opt-out for fundraising	• CEs may not make fundraising communications after opt-out, but may provide method of opting back in.
	CEs may combine "conditioned" and "unconditioned" authorizations for research to simplify authorization paperwork.	• The authorization must differentiate between these two portions. • Unconditioned authorization must be opted in.
	There is a new interpretation on authorization for future research.	• Authorization may be used for future research, with notice to individuals.
	The Final Rule changes access to student immunization records.	• CEs may release immunization records to schools without an authorization that meets HIPAA standards.
	Decedents' PHI is under HIPAA protection for 50 years after death. Covered entities also have greater flexibility to disclose PHI to persons involved in a decedent's care or payment.	• The Final Rule enables CEs to continue communicating with relevant family and friends after an individual's death.
	New definition of marketing includes remuneration from a third party for describing their product or service.	• Covered entities must obtain authorization for third-party marketing.
	Genetic information is now considered PHI.	• Health plans may not use or disclose genetic information for underwriting purposes.

The Final Rule upholds the administrative requirements of covered entities and business associates, which include developing policies and procedures for reporting, analyzing, and documenting a suspected breach of PHI, and training workforce members on these policies and procedures. With the revised definition of a breach, however, the Final Rule notes that covered entities will need to update policies and procedures and retrain their workforce to reflect these new changes.

State vs. Federal Laws

Another key outcome of the revised breach definition and the risk assessment requirement in the Final Rule is that federal and state breach notification laws are more in sync. Most states already require a risk assessment to determine the probability that PHI was compromised. The Final Rule clarifies that only contrary state laws are to be preempted by the federal breach law. This should help covered entities and business associates create a consistent risk assessment approach to ensure compliance with both HIPAA-HITECH and state breach laws.

Risk Assessments: More Critical Than Ever

The Final Rule requires entities to conduct risk assessments to determine if notification is required based on the probability that PHI has been compromised.

But, as the Final Rule points out, risk assessments should already be routine following any security incident.

Covered entities and their business associates should establish a reproducible, consistent process for conducting and documenting risk assessments that incorporates the four elements described in the new legislation.

Business Associates

The HIPAA Final Omnibus Rule extends the definition of a business associate as one that "creates, receives, maintains, or transmits" PHI on behalf of a covered entity. This definition encompasses subcontractors that manage PHI and specific categories of organizations, namely:

- Health information organizations (HIOs)
- E-prescribing gateways
- Patient safety organizations
- Vendors of PHI that provide services on behalf of a covered entity
- Data storage vendors that maintain PHI even if their access to PHI is limited or nonexistent.

Organizations that fit the definition of a conduit are not considered business associates. The Final Rule defines a conduit as one that provides courier services for paper records and data transmission services for electronic PHI; examples include the U.S. Postal Service, the United Postal Service, or Internet service providers (ISPs). The conduit exception applies to these entities because their services are considered "transient" rather than "persistent."

Under the Final Rule, business associates retain the same liability for compliance with certain — not all — HIPAA provisions as covered entities. They are also subject to civil money penalties for HIPAA violations.

Subcontractors as Business Associates

Subcontractors are now bound to the same requirements of the HIPAA Rules as other business associates. According to Adam Greene, a partner at Davis, Wright, and Tremaine, a firm that specializes in privacy and security matters, business associates and their subcontractors must create and implement HIPAA compliance programs. "This includes performing (or revisiting) their risk analysis and risk management processes, developing and implementing appropriate policies and procedures, and training workforce," he says. [5]

Business Associate Contracts

Under the Final Rule, covered entities must enter into a contract with all business associates but they are not required to enter into direct contracts with subcontractors of their business associates and other downstream entities. The same chain of contracts applies. These contracts must specify compliance with the Breach Notification Rule and specify to whom the business associate provides electronic access to PHI. If a covered entity designates HIPAA responsibility to a business associate, the contract must also specify that the business associate will comply with HIPAA regulations.

In addition, contracts in place before January 25, 2013, that do NOT come up for renewal before March 2013 have until September 2014 to come into compliance. All other contracts must abide by the September 23, 2013, deadline.

Increased Enforcement of Willful Neglect

Under the Final Rule, the Office for Civil Rights will step up its enforcement of willful neglect, including investigating all cases of

5. New Omnibus Rule Released: HIPAA Puts on More Weight," Davis Wright Tremaine Advisory by Rebecca L. Williams, Adam H. Greene, Louisa Barash, Jane Eckels, Edwin D. Rauzi, Kent B. (Bernie) Thurber, and Kristen R. Blanchette, January 23, 2013

possible willful neglect. OCR will impose a penalty on all violations of willful neglect, with greater discretion to penalize without seeking informal resolution. Fines could total $1.5 million.

Patient Rights / Use and Disclosure of PHI

The Final Rule reiterates the importance that healthcare providers meet stringent requirements for patient privacy and data security. OCR has aggressively increased its enforcement toward organizations with lax privacy and security, with stiff penalties for noncompliance.

The most significant clarification in the Final Rule in this regard is related to patient access. Patients will now have the right to get electronic copies of all of their electronic medical records upon request. In the past, providers' policies in this area have varied significantly.

Rulings that favor restricting access to PHI include:

The right to restrict disclosures of a patient's medical information to their health plan, if they pay for a service or item in full.

Written and signed request by individual is required for third-party access to PHI.

A ban, with exceptions, on the sale of PHI without authorization. This ban applies to limited data sets.

New limits on how PHI is used and disclosed for marketing. This includes receiving remuneration for describing a third-party item or service — even if the manufacturer or service provider paid for the communication.

Health plans may not use or disclose genetic information for underwriting purposes.

Other provisions in the Final Rule favor increased access to PHI:

New categories of PHI may be used or disclosed for fundraising. Greene notes that this enables healthcare organizations to better target fundraising efforts.

The right to combine "conditioned" and "unconditioned" authorizations for research, simplifying authorization paperwork. In addition, one-time authorization may be applied, with notice, for future research.

Student immunizations may be released to schools without satisfying HIPAA authorization requirements.

HIPAA protections apply to decedents' PHI for a limit of 50 years after death. As Greene notes, the Final Rule also offers greater flexibility regarding the disclosure of a decedent's PHI to those involved in that patient's care or payment.

Covered entities will be required to change their notice of privacy practices to reflect these new rulings.

Planning for Compliance: How to Take Action Now

The Final Rule puts renewed pressure on covered entities and business associates to act now to achieve compliance with HIPAA and breach notification requirements. With greater enforcement by OCR, healthcare organizations also need to demonstrate and document this compliance. ID Experts recommends five immediate steps to provide a solid and comprehensive foundation for compliance with these regulations:

What Are Business Associates Liable For?

- Impermissible uses and disclosures
- Breach notification to covered entity
- Failure to provide electronic copies of ePHI as specified in the business associate contract
- Failure to disclose PHI to HHS for HIPAA investigations
- Failure to provide an accounting of disclosures
- Failure to comply with the applicable requirements of the HIPAA Security Rule

Carry out and document annual privacy and security risk assessments. These should reflect "vulnerabilities addressed in HHS guidance, such as mobile devices."[6]

Clearly identify, manage, and document compliance of business associates and their downstream subcontractors.

Define and document your method for the security incident risk assessments that determine if an incident is a reportable breach or not.

Document your policies and processes for complying with the limiting of access to patient information for marketing or other purposes where a patient can restrict access.

Take advantage of the safe-harbor provision by encrypting PHI according to NIST specifications. Breaches of properly encrypted PHI are generally exempt from notification.

Given the time and effort it takes to achieve compliance, it helps to have tools in place to support your plan. ID Experts offers complete data breach care, from proactive prevention to objective analysis to

6. New Omnibus Rule Released: HIPAA Puts on More Weight," Davis Wright Tremaine Advisory by Rebecca L. Williams, Adam H. Greene, Louisa Barash, Jane Eckels, Edwin D. Rauzi, Kent B. (Bernie) Thurber, and Kristen R. Blanchette, January 23, 2013

caring, compliant incident response. For healthcare organizations, we provide a Healthcare Incident Response Plan to help establish a documented plan before an incident. RADAR™, our online incident management software, is an award-winning tool for performing incident risk assessments as prescribed in the Final Rule.

Fostering A "Culture of Compliance"

The HIPAA Final Omnibus Rule seeks to better protect patients' privacy while giving them greater control of their personal health information. At the same time, it strengthens OCR's ability to enforce the law. In our experience, organizations that aim for voluntary compliance — what OCR calls a "culture of compliance" — have little to fear from regulators. All of the policies and procedures, training, privacy and security measures, and response plans — all these should be implemented with an eye toward protecting the patient's physical and reputational wellbeing. Seek to do well by your patients, and compliance will follow.

Don't Forget Training!

The HSSA/SCCE survey found that the leading source (38%) of breach incidents is due to lost paper files and that the leading source of discovery of these incidents is from non-IT employees.[7] This suggests that data security and patient privacy issues are closely linked to policies and procedures and employee training.

7. See "Health data breach trends from HCCA, SCCE survey, " January 25, 2013, HealthITSecurity.com.

Learn more online

www.IDExpertsCorp.com

@IDExperts

All Things HITECH
All Things Data Breach

id experts®

About ID Experts

ID Experts® provides software and services to simplify the complexities of managing privacy and security incident response. Its award-winning RADAR™ software is relied on by some of the largest healthcare, insurance, and financial services organizations to reduce risks and ensure compliance. For more than a decade, ID Experts has provided data breach services and managed thousands of incidents. Endorsed by the American Hospital Association, ID Experts is an advocate for privacy and participates with the Consumer Federation of America, the PHI Protection Network and Patient Privacy Rights.