DOWNLOADABLE GUIDE

HIPAA Final Omnibus Rule Playbook

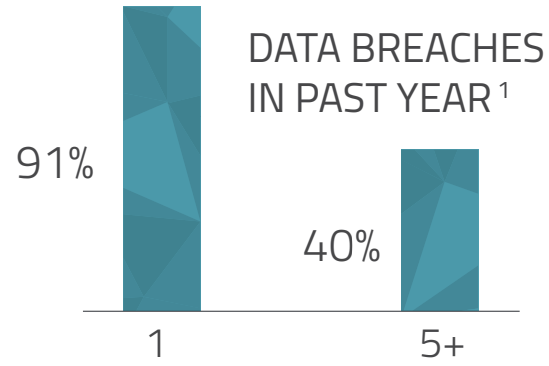
Your Ticket to Winning the Compliance Game

Offensive Plays
HIPAA Privacy Rule

Defensive Plays
HIPAA Security Rule

Special Team Plays
Breach Notification Rule

Additional Plays



Data breaches risk the medical and financial well-being of your patients (or members if you are a health plan), and the credibility and future business of healthcare organizations.

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 protected health information (PHI) breach epidemic. The most sweeping of these regulations is the long-awaited HIPAA Final Omnibus Rule.

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 reflects landmark legislation that affects nearly every aspect of patient privacy and data security. It encompasses a number of changes, including:

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

HIPAA covered entities (CEs) must overcome daunting challenges — lack of time, resources, and expertise — to win the compliance game. With HHS Office for Civil Rights imposing more severe penalties for violations, covered entities need to take the offensive and plan for victory now. The coaching staff at ID Experts assembled this comprehensive playbook to guide privacy and information security professionals to compliance. The "plays" we've developed encompass all major aspects of the Final Rule — HIPAA-HITECH Privacy, Security, and Breach Notification Rules — and how you need to manage your business associates based on new guidelines.

We've chosen these plays to help covered entities with limited time and resources identify key aspects of the Final Rule and plan for compliance. The checklist below outlines the requirements of the Final Rule and the plays you should make to protect your team, avoid penalties, and win the compliance championship.

Let the Games Begin!

"This Final Omnibus Rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes…strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."*

— Leon Rodriguez, Former Director of HHS Office for Civil Rights

* "BREAKING: HHS Releases HIPAA Update," Healthcare Informatics, January, 17 2013
1 "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data" by Ponemon Institute, May 2016.

id experts®

Offensive Plays — HIPAA Privacy Rule

Use the list of requirements below to strategize your compliance with the HIPAA Privacy Rule.

Background

To help protect against the breach of personal medical information, the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, set standards for medical privacy that went into effect over the next 10 years. 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. It imposed new requirements, including extension of the HIPAA Privacy and Security Rules to include business associates, a tiered increase in penalties for violations of these rules, and mandatory audits by HHS. The HIPAA Final Omnibus Rule implements certain provisions of the HITECH Act to "strengthen" the protections of the Privacy and Security Rules.

HIPAA Privacy Rule

According to HHS, "a major goal of the [HIPAA] Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and well-being."[2]

Training

HHS requires periodic privacy and security training for all employees of healthcare organizations. This is critical, given that a Ponemon Institute found that the leading source of breach incidents is criminal attacks and that the leading source of discovery of these incidents is from internal audit/assessment.[3] This suggests that data security and patient privacy issues are closely linked to policies and procedures, and employee training.

Workforce training	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

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. Some of the new requirements favor increased access to PHI, while others restrict access. Either way, covered entities must update their policies and procedures to reflect the Final Rule's mandates regarding the use and disclosure of PHI.

Update policies and procedures regarding the use and disclosure of PHI for the following:

Fundraising New categories of PHI may be used or disclosed for fundraising, enabling covered entities to better target fundraising efforts.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Data Breaches: The Everyday Disaster

According to the Sixth Annual Benchmark Study on Patient Privacy & Data Security by Ponemon Institute, 90% of healthcare organizations suffered data breaches, costing the healthcare industry an average of $6.2 billion a year.

2 "Summary of the HIPAA Privacy Rule," Department of Health and Human Services (hhs.gov).
3 "Sixth Annual Benchmark Study on Patient Privacy & Data Security," by Ponemon Institute, May 2016.

id experts®

Marketing The Final Rule redefines marketing to include receiving remuneration from a third party for describing their product or service. CEs must obtain authorization for third-party marketing.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Designated third-party receipt of PHI Requests must be made in writing, and clearly identify the recipient and where to send the PHI.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Ban on sale of PHI The Final Rule prohibits, with exceptions, the sale of PHI without authorization. This ban applies to limited data sets.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Restrictions on disclosure when paid in full 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.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Disclosure of genetic information for underwriting purposes Health plans may not use or disclose genetic health information for underwriting purposes.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
School immunizations CEs may release immunization records to schools without an authorization if done pursuant to HIPAA standards.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Decendent Information Decedents' PHI is under HIPAA protection for 50 years after death. The Final Rule enables CEs to continue communicating with relevant family and friends after an individual's death.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Privacy Notices

Covered entities must change their privacy notices to reflect new privacy practices and patient rights. Update notice pf privacy practices to include:

Prohibition of sale of PHI	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Duty to notify in case of a breach	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

"If you handle protected health information, you may be able to get by without understanding the details of health reform, but you cannot survive in your job if you do not understand and comply with the HIPAA/HITECH rules. Anyone involved in the health care business who does not comply with these laws is a walking liability."

— James C. Pyles
Principle, Powers, Pyles, Sutter & Verville PC

id experts®

Right to opt out of fundraising	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Right to disclosure restrictions when paid in full	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Limit on use of genetic information	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Electronic Copies of PHI

Patients now have the right to get electronic copies of all of their electronic medical records upon request, rather than a hard copy, even if the electronic copy is not readily reproducible. Patients can also direct that a designated third party receive copies.

Provide a method for patients to receive electronic copies of electronic PHI.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Research

HHS finalized its proposal to allow a blending of "conditioned" and "unconditioned" authorizations for research into a single document, where individuals can simply opt-in to the unconditioned authorization.

In addition, one-time authorization may be applied, with notice, for future research. "The language of the authorization must adequately inform the individual that the individual's PHI may be used in future research studies," says Adam Greene, a partner at Davis, Wright, and Tremaine, a firm that specializes in privacy and security matters.

Update research authorization policies/paperwork to:

Allow for combined "unconditioned" and "conditioned" authorizations.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Allow for authorizations for future research, with notice, to individuals.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Defensive Plays — HIPAA Security Rule

Use the list of requirements below to strategize your compliance with the HIPAA Security Rule.

Background

According to HHS, "the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[4] Under the Final Rule, business associates are also bound to provisions of the HIPAA Security Rule.

Assessment of Secuirty Risks

Assess and document risks to PHI relative to regulatory obligations, and develop and implement mitigation strategies for achieving compliance.

Perform a HIPAA security compliance assessment. A HIPAA security compliance assessment evaluates a CE's regulatory obligations; existing administrative, technical and physical safeguards; and gaps along with recommendations for ensuring regulatory compliance and best practices.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Conduct a security risk analysis. A risk analysis is a prospective and in-depth analysis of the risks to a covered entity's information assets involving electronic PHI and recommendations to meet the requirements of the HIPAA Security Rule — including updated requirements in the Final Rule. This is also a requirement for meaningful-use attestation by covered entities.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Mitigation and Action

Take proper steps to mitigate the likelihood and impact of a data breach based on the assessment of your organization's security risks.

Develop risk mitigation scope. Review and prioritize the risks revealed by your risk analysis based on their business impact and likelihood of occurrence.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Create a mitigation plan. Develop a risk mitigation plan including prospective schedules for addressing security vulnerabilities and required budgets and resources.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Ensure Your HIPAA Compliance

HIPAA compliance assessments evaluate your regulatory obligations, current level of compliance, and gaps with respect to HIPAA-HITECH Privacy, Security, and Breach Notification Rules, as well as states laws.

Our HIPAA Compliance Assessment service provides an efficient and credible evaluation of your compliance gaps, a priority ranking of your risks, and recommendations for mitigating those risks.

Best practice suggests a HIPAA compliance assessment should be conducted annually.

Contact us to learn more about ID Experts' HIPAA Compliance Assessment service

4 http://www.hhs.gov/hipaa/for-professionals/security/

id experts®

Update relevant security policies and procedures. Revisit and update security policies and procedures for these high-risk items.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Evaluate and implement security technologies. Based on the risk analysis, implement or update safeguards and technologies to protect PHI. Pay special attention to encrypting PHI in all modes — in motion, at rest, etc. according to NIST specifications. Doing so provides a safe harbor from data breach notification requirements in many cases.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Special Team Plays — Breach Notification Rule

Use the list of requirements below to strategize your compliance with the Breach Notification Rule.

Background

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." The HIPAA Final Omnibus Rule removes the harm standard, replacing it with a new compromise standard. However, the Final Rule does not explicitly define the term "compromise." Covered entities 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 risk assessment must include a minimum of these four factors:

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

If your organization has a security or privacy incident involving PHI, and your risk assessment concludes there was a very low probability that PHI was compromised, you may choose to not notify the affected individuals or OCR. However, the Final Rule requires that your organization maintain a burden of proof if your conclusions are called into question — or demonstrate that one of the existing exceptions to the definition of breach applies.

Consider Cyber Insurance

Cyber insurance can help offset the unpredictable costs of data breach response, such as legal liabilities and other "non-tangible" expenses. But not all policies are the same. Find the right coverage for you.

Download the 10 Things to Consider Before Purchasing Cyber Insurance at www2.idexpertscorp.com/resources/single/10-things-to-consider-before-purchasing-cyber-insurance/r-general

id experts®

Policies and Procedures

Update policies and procedures to enable you to:

Detect and escalate a potential breach to your incident response team.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Conduct consistent incident risk assessments per the Final Rule.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Provide supporting documentation to meet your burden of proof, including your incident risk assessment methodology.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Incident Response Planning & Testing

Prepare, document, and test the proper steps for a breach response following a data security or privacy incident that complies with the new breach definition outlined in the Final Breach Notification Rule.

Planning • Update your incident response plan by incorporating your new incident risk assessment methodology and associated updates to your policies and procedures. • Identify methods for detecting a breach. • Determine types of notification based on the level of risk. • Identify the response team and designate roles and responsibilities.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Testing • Retrain your incident response team and workforce members on incident reporting protocol. • Periodically conduct a tabletop or full-scale test and make needed adjustments.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Incident Risk Assessment

Define and document a method for consistent incident risk assessment using the four factors required by the Final Rule. Ensure that your method provides the necessary decision support to determine if an incident is a reportable breach or not and meets your burden of proof obligations under the Final Rule.

Incident Assessment that's Final Rule-Compliant

The Final Rule requires that you carry out an incident risk assessment following every PHI privacy or security assessment. At the same time, the Final Rule removed the controversial "harm standard" and replaced it with what is being called the "compromise standard."

id experts®

Method uses the four factors required by the Final Breach Notification Rule	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Method provides decision support and meets your burden of proof obligations under the Final Breach Notification Rule.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Business Associate Plays

Use the list of plays below to ensure compliance with your business associate contracts.

Background

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 now also 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

Covered entities should review their roster of vendors, service providers, and other third parties and enter into contracts (that include the BA Definition Scope Expansion) with these "new" business associates.

In addition, 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. 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.

New Definition of Business Associates

Prepare, document, and test the proper steps for a breach response following a data security or privacy incident that complies with the new breach definition outlined in the Final Rule.

OCR to Focus on Business Associates

"Despite the requirements of HIPAA, not only do a large percentage of covered entities believe they will not be notified of security breaches or cyber attacks by their business associates, they also think it is difficult to manage security incidents involving business associates, and impossible to determine if data safeguards and security policies and procedure are adequate to respond effectievly to a data breach."[5]

[5] "Is Your Business Associate Prepared for a Security Incident?" OCR Cyber-Awareness Monthly Update, May 3, 2016

Create new contracts with entities that fit the new definition of a business associate.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Update Business Associates Contracts

These contracts must specify:

Compliance with the Breach Notification Rule	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Liability for HIPAA compliance	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Assurances that they and subcontractors will safeguard PHI	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

On to Victory!

The HIPAA Final Omnibus Rule impacts nearly every aspect of a covered entity's patient privacy and data security measures. But with this playbook, winning the compliance game doesn't have to be daunting. And you don't have to go it alone. Your coaching staff at ID Experts will be on the sidelines guiding you to victory, every step of the way.

Talk to an expert

971-242-4775 | Info@IDExpertsCorp.com

id experts®

About ID Experts

At ID Experts, we provide innovative software and services that simplify the complexities and reduce the risks of managing data incident response. Since 2003, we have served many of the largest healthcare, financial services, retail, and government organizations in the U.S.

Helpful Resources & Information

Blogs

Text of the HIPAA Final Omnibus Rule
www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Protected Health Information (PHI) Project
ANSI/Shared Assessments/Internet Security Alliance
webstore.ansi.org/phi

HHS/OCR Data Breach Site (AKA the "Wall of Shame")
http://www.hhs.gov/hipaa/for-professionals/security/

HIPAA/HITECH Privacy/Security & Breach Notification
HHS/OCR Administrative Simplification Statue and Rules
www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

ID Experts Corporate Blog
www2.idexpertscorp.com/blog

PHI Privacy Blog
www.phiprivacy.net

All Things HITECH — LinkedIn Group
Join the conversation about privacy, healthcare, and compliance in the All Things HITECH Group.
www.linkedin.com/groups/All-Things-HITECH-3873240

Research/Papers

Sixth Annual Benchmark Study on Privacy & Security for Healthcare Data, Ponemon Institute, May 2016
www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents

The HIPAA Final Omnibus Rule: An Analysis of The Changes Impacting Healthcare Covered Entities and Business Associates, February 2013
www2.idexpertscorp.com/resources/single/hipaa-final-omnibus-rule-whitepaper/r-data-breach-response

Sixth Annual Survey on Medical Identity Theft
Ponemon Institute, February 2015
http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

2016 Data Breach Investigations Report
Verizon Business
http://www.verizonenterprise.com/DBIR/2016/

Products & Services

Risk Assessment Services
MIDAS™—Medical Identity Alert System—is the first and only member-focused healthcare fraud solution that engages health plan members to monitor their healthcare transactions and take control of their medical identities
www2.idexpertscorp.com/midas-software

Healthcare Data Breach Solutions
Protect your patients and your organization with our comprehensive breach prevention and response services.
www2.idexpertscorp.com/data-breach-solutions/healthcare

Cyber Insurance Checklist
www2.idexpertscorp.com/resources/single/10-things-to-consider-before-purchasing-cyber-insurance/r-general

About This Document

Please realize that the HIPAA Final Omnibus Rule is very lengthy and detailed. While this document and its checklists are intended to provide you with guidance as to general, high-impact best practices that will assist in preparing for compliance, they are not intended to be exhaustive as far as all of your privacy, security, and breach notification obligations under the Final Rule. This information is not intended to be or replace legal advice. Please seek out your legal counsel for such advice.

id experts®