id experts®

DOWNLOADABLE GUIDE

HIPAA Final Omnibus Rule Playbook for Business Associates

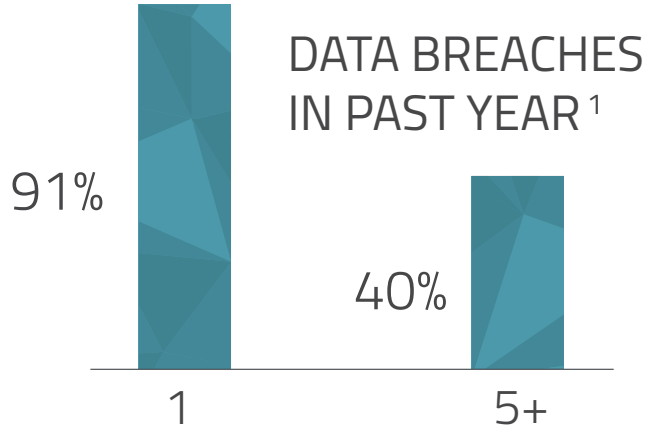
Your Ticket to Winning the Compliance Game

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 patients, 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 requirement
- 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

Business Associates and the Final Rule

The Final 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 also encompasses subcontractors that manage PHI and specific categories of organizations, namely:

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

"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®

Business associates—whether existing or new—face many of the same compliance requirements as their covered entities, making them subject to regulatory fines and corrective action plans, as well as civil money penalties and lawsuits. In addition, OCR includes business associates in its HIPAA compliance audits. Business associates must demonstrate their compliance and meet their contractual obligations with covered entities. And, as Kirk Nahra a partner at Wiley Rein points out, organizations should understand that they could be a business associate by legal definition, even without a business associate contract with a covered entity or another business associate.[2]

With these liabilities, business associates need to take the offensive and plan for victory now. The coaching staff at ID Experts assembled this comprehensive playbook to help 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 business associates need to manage their agreements with covered entities and subcontractors based on new guidelines.

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!

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."[3]

Data Breaches: The Everyday Disaster

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

2 "The New HIPAA/HITECH Era Is Finally Here," Privacy in Focus, Kirk J. Nahra of Wiley Rein LLP, February 2013.
3 "Summary of the HIPAA Privacy Rule," Department of Health and Human Services (hhs.gov).

id experts®

Training

HHS requires healthcare organizations to provide periodic privacy and security training to all workforce members. 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. [4] This suggests that data security and patient privacy issues are closely linked to policies and procedures, and employee training. Training may be supplemented with a system of sanctions for violations of the entity's policies.

Provide workforce training	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Implement employee sanctions	◯ 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.

Generally, BAs may only use or disclose PHI in the same manner as a covered entity. Thus, any Privacy Rule limitation on how a covered entity may use or disclose PHI automatically extends to a business associate. In the past, BAs only had contractual obligations and had to comply with the terms of a business associate agreement related to the use and disclosure of PHI. With the publication of the Final Rule, however, BAs must comply with most provisions of the Privacy Rule.

Limited Data Sets/Minimum Necessary Keep the disclosure of PHI to limited data sets or minimum necessary to accomplish the intended purpose of the use, disclosure, or request.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Restrictions on disclosure when paid in full BAs 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 PHI to HHS BAs must provide PHI to the Secretary of HHS upon demand.	◯ 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

4 "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," by Ponemon Institute, May 2016.

id experts®

Subcontractors
Enter into business associate agreements, which include reasonable assurances about safeguards, with subcontractors that create, receive, maintain, or transmit PHI on your behalf.

- ◯ Automated / Optimized
- ◯ Hybrid / Adequate
- ◯ Manual / Ineffective

Ban on sale of PHI
The sale of PHI is prohibited unless authorized by the individual.

- ◯ Automated / Optimized
- ◯ Hybrid / Adequate
- ◯ Manual / Ineffective

Marketing
The Final Rule redefines marketing to include receiving remuneration from a third party for describing their product or service. BAs must obtain authorization for third-party marketing.

- ◯ Automated / Optimized
- ◯ Hybrid / Adequate
- ◯ Manual / Ineffective

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

Designated third-party receipt of PHI
Requests must be made in writing, and clearly identify the recipient and where to send PHI.

- ◯ 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

Decedent 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

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

Accounting and Disclosure of PHI to Covered Entities

The HIPAA Final Omnibus Rule does not change the requirements regarding the accounting and disclosure of PHI to covered entities. Business associates must comply with the Privacy Rule's existing accounting and disclosure requirements. In addition, the HITECH Act requires BAs to provide an accounting of disclosures to individuals who request such an accounting.

Provide a method for tracking and documenting disclosures of PHI to the covered entity. These disclosures include those made in the previous section: "Use & Disclosures of PHI."	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Privacy Notices of Covered Entities

Although there are no regulatory requirements, business associates may be contractually required to display the updated privacy notices of their covered entities. These updates must reflect new privacy practices and patient rights as outlined in the Final Rule.

Display updated privacy notices of covered entities onsite and online.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Electronic Copies of PHI

Patients now have the right to receive 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 an electronic copy of PHI to the covered entity, the individual, or the individual's designee as specified in the BAA.	◯ 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.

BAs must comply with the terms of a business associate agreement related to the authorization of PHI in research:

"Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program."

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

** OCR/NIST 6th Annual Conference
Safeguarding Health Information: Building Assurance through HIPAA Security, May 22, 2013

id experts®

Allow for combined "unconditioned" and "conditioned" authorizations.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Allow for authorizations for future research, with adequately explained 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."[5]

Under the requirements, business associates and their applicable subcontractors must comply with the full HIPAA Security Rule. "This is a significant additional step in security compliance that will affect an enormous number of business associates," says attorney Kirk Nahra.[6]

Assessment of Security 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. This assessment evaluates: • A BA's regulatory obligations • Existing administrative, technical, and physical safeguards • Gaps along with recommendations for ensuring regulatory compliance and best practices. This will help prepare BAs for OCR audits and contractual compliance with covered entities.	◯ 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. Best practice suggests a HIPAA compliance assessment should be conducted annually.

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.

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

5 "The Security Rule," Department of Health and Human Services (hhs.gov).
6 "The New HIPAA/HITECH Era Is Finally Here," Privacy In Focus, Kirk J. Nahra of Wiley Rein LLP, February 2013.

id experts®

Conduct a security risk analysis.
A risk analysis is a prospective and in-depth analysis of the risks (vulnerabilities and threats) to a business associate's information assets and business processes involving electronic PHI.
It includes recommendations to meet the requirements of the HIPAA Security Rule — including updated requirements in the Final Rule. This play addresses a key part of the OCR audits, and helps meet a requirement 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

Update relevant security policies and procedures.
Revisit and update security policies and procedures for these high-risk items. Include procedures for reporting to CEs uses or disclosures of PHI that are not provided in the BAA and do not rise to the level of a security breach.

- ◯ Automated / Optimized
- ◯ Hybrid / Adequate
- ◯ Manual / Ineffective

Create a mitigation plan.
Develop a risk mitigation plan including prospective schedules for:

- Determining which security measures are "reasonable and appropriate."
- Creating and implementing effective security measures.
- Assessing and updating existing security measures, and required budgets and resources.

- ◯ 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, including portable storage devices such as smartphones, tablets, 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

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

id experts®

Special Team Plays — Breach Notification Rule

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

Background

Under the breach notification 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 Final Breach Notification 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 and business associates must still conduct an incident risk assessment for every data security incident that involves PHI because a breach is now presumed. Rather than determine the risk of harm, however, the risk assessment determines the level of probability that PHI has been compromised, and if so, then notification is required. 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 a business associate has a security or privacy incident involving disclosure of unsecured PHI/ePHI to an unauthorized recipient, it needs to conduct a risk assessment based on the above factors. The business associate must notify its covered entities of the incident and the results of the risk assessment — in other words, provide all the information necessary for notification, as well as for HHS/OCR reporting and investigation. It must maintain a burden of proof if its conclusions are called into question — or demonstrate that one of the existing exceptions to the definition of a breach applies.

Notification

If a business associate has agreements with multiple covered entities, a breach may affect more than one CE, creating complex legal obligations and notification of those entities. The following checklist can help.

Notify all affected covered entities as required by § 164.410 and based on BA agreement timelines, and provide covered entities the necessary information they need to meet regulatory obligations.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Notify affected individuals if this requirement is contractually specified in the BA agreement. Regardless, the CE remains legally responsible.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

Limited Data Sets/Minimum Necessary
Keep the disclosure of PHI to limited data sets or minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- ◯ Automated / Optimized
- ◯ Hybrid / Adequate
- ◯ Manual / Ineffective

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 as per the four factors specified in the Final Breach Notification Rule.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Provide supporting documentation to meet your burden of proof, including your compliant 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

- Designate an incident response team, including a core team and an extended team.
- Identify internal and external resources (forensics and response vendors).
- Designate roles and responsibilities.
- Update your incident response plan, if one exists, by incorporating your new incident risk assessment methodology and associated updates to your policies and procedures.
- Identify methods for reporting and escalating a suspected breach incident to the core response team.
- Train the response team on incident risk assessment methodology, and how to execute the plan

◯ 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 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®

Incident Risk Assessment

Define and document a method for consistent incident risk assessment using the four factors required by the Final Breach Notification 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 Breach Notification Rule.

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

Additional Plays — Dealing with Covered Entities, Regulators, and Subcontractors

Regulators and Covered Entities

The increased focus on business associates can be intimidating. But former OCR Director Leon Rodriguez has assured both CEs and BAs that the regulator isn't in the game of "gotcha." Organizations that take proactive measures won't be punished for a one-time incident. He acknowledged the inevitability of data breaches, and said OCR's focus is on organizations that consistently fail to comply with the HIPAA Privacy and Security Rules, including a failure to conduct risk analyses.[7] Business associates' efforts in achieving compliance will include meeting the legal requirements outlined in the agreements they have with covered entities.

Understand your agreement with covered entities. • Ensure the contract/agreement is up to date to meet the Final Rule requirements. This includes a discussion on how to implement these requirements into the contract,[8] and strikes any old BAA language that may have exempted BAs from their new obligations. • "Develop a contracting process and approach for now and over the next 2 years."[9]	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Implement policies and procedures to meet those updates and track your compliance, etc.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
Provide documentation to show compliance with applicable Privacy, Security, and Breach Notification Rules. CEs and possibly regulators may request this.	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

OCR to Focus on Business Associates

According to Leon Rodriguez, Former Director of HHS Office for Civil Rights, 63% of those affected by healthcare data breaches reported to OCR were a result of a security breach at a business associate rather than a covered entity.

7 "HHS OCR director Leon Rodriguez's dialogue on HIPAA/HITECH compliance," by Kimberly M. Wong, BakerHostetler, May 23rd, 2013, Lexology.com
8 See "The New HIPAA/HITECH Era Is Finally Here," Privacy In Focus, Kirk J. Nahra of Wiley Rein LLP, February 2013
9 Ibid.

id experts®

Subcontractors

Under the Final Rule, subcontractors are now bound to the same requirements of the HIPAA Rules as their business associates. BAs must enter into direct contracts with their subcontractors and other downstream entities, maintaining the chain of "satisfactory assurances" that starts with CE-BA agreements. However, a business associate is held liable if it knew of a subcontractor's pattern of conduct, and did not take reasonable steps to stop the breach or violations.

Understand your options if there is a breach on the part of a subcontractor or other downstream entity:

Does the agreement allow the business associate to find another provider, if feasible?	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective
If the subcontractor is the only provider of that service, what recourse does the business associate have?	◯ Automated / Optimized ◯ Hybrid / Adequate ◯ Manual / Ineffective

On to Victory!

The HIPAA Final Omnibus Rule impacts nearly every aspect of a business associate'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

BAs and Subcontractors as Agents

According to the Final Rule, an "agency relationship exists between a covered entity and its business associate (or BA and its subcontractor)" if it has "the right or authority…to control the business associate's conduct in the course of performing a service on behalf of the covered entity."

Covered entities and business associates may be liable for the actions of their business associate agents, even if they have a business associate agreement. Kirk Nahra, a partner at Wiley Rein LLP, stresses the importance of evaluating the "agent idea."

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")
www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

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 of Healthcare Data, Ponemon Institute, May 2016
www2.idexpertscorp.com/ponemon2016

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

Fifth Annual Survey on Medical Identity Theft
Ponemon Institute, February 2014
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

Virtual Privacy Expert™
The Virtual Privacy Expert is an easy-to-use web portal that provides organizations with real-time feedback and useful resources to help protect themselves from data breach risks.
www2.idexpertscorp.com/data-breach-response/virtual-privacy-expert

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

10 Things to Consider Before Purchasing Cyber Insurance
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®