Stericycle®

WHITE PAPER

HIPAA COMPLIANCE: 6 REALITY CHECKS

Mitigate the Risk of a Breach or HIPAA Violation

www.Stericycle.com/HIPAA • 866-783-9814

TABLE OF CONTENTS

HIPAA COMPLIANCE: 6 REALITY CHECKS

Mitigate the Risk of a Breach or HIPAA Violation

INTRODUCTION

The Challenges

Your obligation to safeguard both the privacy and security of patient information, is not something you take lightly. But that "balancing act between maintaining security and not inhibiting the business"[1] continues to challenge many privately owned and smaller providers. Performance audits[2] have shown too many organizations are not allocating sufficient time and resources to stay in compliance with HIPAA regulations and to mitigate the risk of ePHI (electronic protected health information) and paper record breaches.

The typical person tasked with responsibility to manage HIPAA compliance within a covered entity health care provider with annual revenue less than $50 million has limited bandwidth and competing priorities. Investing sufficient time and effort to accomplish all the activities that HIPAA requires is a challenge; and/or the support and tools needed to effectively oversee and sustain compliance don't exist at their facility.

Making matters worse, the HIPAA Omnibus Rules have created additional requirements that make compliance more complex and time-consuming — even for the most conscientious and productive compliance officers.

Finding a Solution

As compliance requirements continue to become more involved, your organization must make an ongoing investment in proactively mitigating the risk of a HIPAA violation or PHI breach. It's crucial that your organization achieves and maintains compliance relating to workforce education, proper documentation management, continual risk analysis, and ongoing monitoring.

The costs resulting from a PHI breach — financial, legal, operational, and clinical repercussions and the damage to your reputation — can devastate your organization. It's up to you to mitigate your risk by taking charge and demanding a culture of compliance. If you need extra support, or the inefficiency of trying to "do it alone" has exposed you, the easiest way to stay in compliance is to engage a qualified third-party provider who can help you develop an ongoing HIPAA compliance program.

It's Time for 6 Reality Checks.

REALITY CHECK

1 DATA BREACHES ARE A CONSTANT THREAT

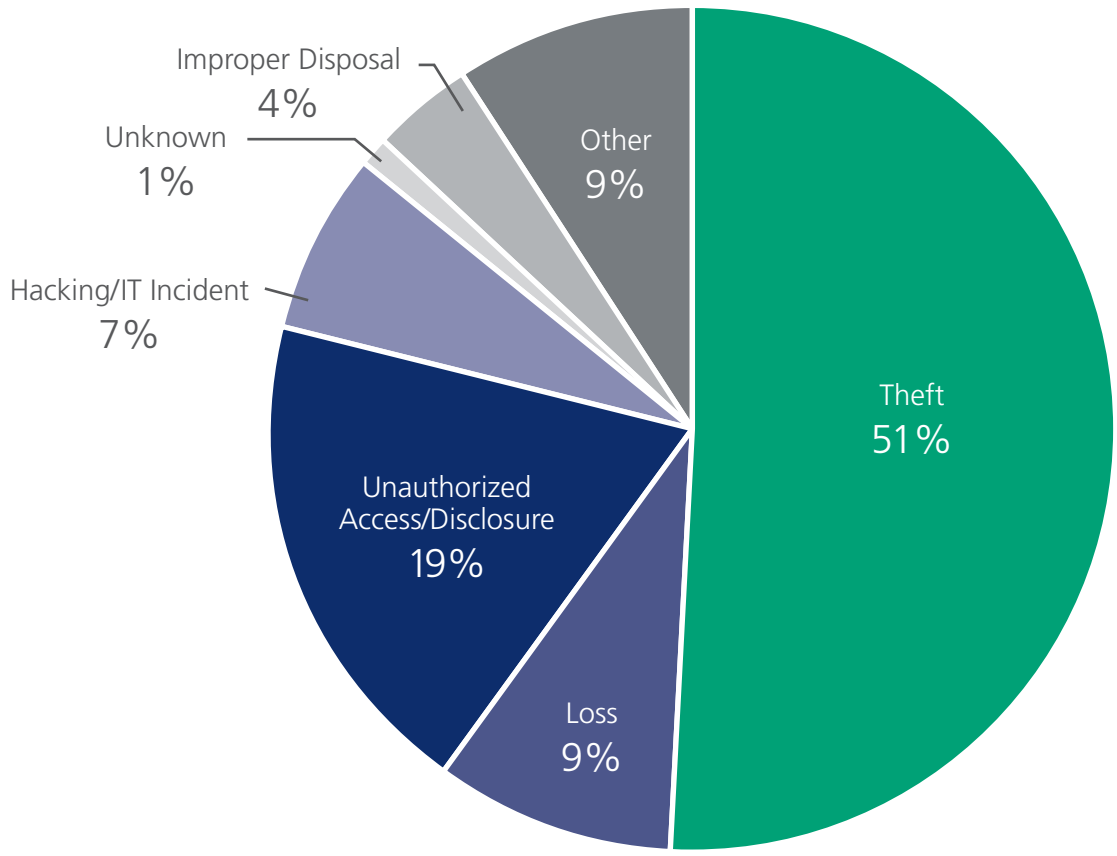
At the 2015 National HIPAA Summit, Director Jocelyn Samuels, U.S. Department of Health and Human Services Office for Civil Rights (OCR), reported there have been approximately 1,144 major health care data breaches involving the PHI of 500 or more individuals. These breaches resulted in the exposure of the personal health care data of over 41 million patients. Additionally, from September 2009 through February 2015, there have been 157,000 reported breaches involving the PHI of fewer than 500 individuals.[3]

OCR breach report statistics have shown that covered entities of every size are to blame. Major breaches occur in both large and small provider organizations. It can happen to you. The threat is constant. That's why it's crucial that you be fully aware of the potential risks and take proactive steps to protect your patients' health information and your business.

OCR breach report statistics have shown that covered entities of every size are to blame. Major breaches occur in both large and small provider organizations.

Leading Causes of Major Breaches by Type

(500+ individuals impacted)



[a] Samuels, U.S. Department of Health and Human Services, Office for Civil Rights. Data presented at 23rd National HIPAA Summit as of February 27, 2015.

Theft (51%)

According to OCR data as of February 2015, 51% of all major breach events (those impacting 500 or more individuals) were due to theft of unsecured protected health information (PHI). This is not a new trend. Historically, over 50% of the major data breaches publically displayed on the HHS.gov website stem from stolen unencrypted computing devices, network servers, storage media and other mobile devices, in addition to traditional paper records containing PHI.

Identity theft now tops the list of consumer complaints that are reported to the FTC and other enforcement agencies every year — and reports of medical identity theft are rising.

This type of theft can involve someone stealing or misusing personally identifiable information (PII), such as name and Social Security number, credit card numbers, financial account information along with health information, and insurance coverage. The more information a thief can obtain, the more valuable it is.

An estimated 1.84 million people were victims of medical identity theft in 2013 according to the Ponemon Institute.[4]

While most of the leading breach locations are related to computers and other information technology, a full 22% of breaches involve paper records.[3]

Unauthorized Access or Disclosure (19%)

In one reported breach incident, a health care provider was notified that a business associate, a medical transcription service, had a server compromised. The PHI detailing Medicaid ID numbers, dates of birth, and names of primary physicians could be viewed online.

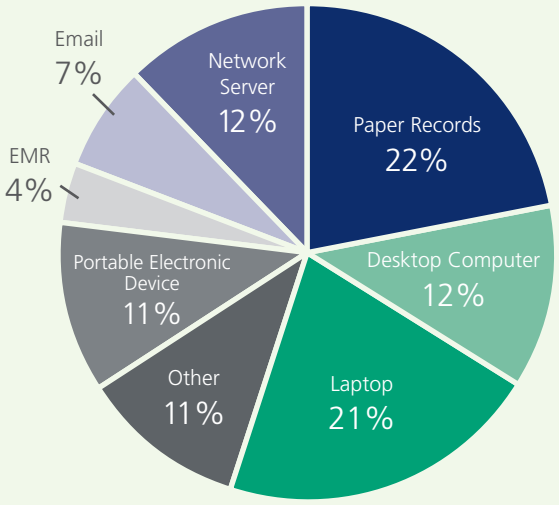
Loss (9%)

In another incident, an employee lost a laptop while in transit on public transportation. The laptop contained PHI that included names, Medicaid ID numbers, dates of birth, and names of primary physicians.

Hacking or Other IT Incident (7%)

Technology can help mitigate security risks. However, it can also be an area of vulnerability. One incident of a computer server breach resulted in the disclosure of 27,000 prescription records to unauthorized parties. The PHI included names, addresses, diagnostic codes, name of medication prescribed, medication costs, and some Social Security numbers.

Leading Locations of Breaches



500+ Breaches by Location
Data as of February 2015

[a] Samuels, U.S. Department of Health and Human Services, Office for Civil Rights.

Improper Disposal (4%)

Safeguarding PHI includes the proper disposal of paper and electronic records. One investigation concluded that the covered entity improperly disposed of patient demographic, financial, clinical, and other medical information by placing the PHI in a dumpster outside of a doctor's office.

REALITY CHECK 2

OCR AUDITS REVEAL THAT HEALTH CARE PROVIDERS ARE NOT IN COMPLIANCE

In 2011 and 2012, OCR conducted privacy (including breach) and security performance audits of covered entities, as required by the HITECH Act audit mandate. These audits analyzed key processes, controls, and policies of the audited organizations relative to HIPAA regulations and provided findings or observations.

Audit Goal: Improve Compliance

The goal of OCR's Audit Program is to improve covered entity compliance with HIPAA standards by:

- Examining compliance programs and mechanisms used;
- Identifying best practices;
- Discovering risks and vulnerabilities occurring across all types of HIPAA covered entities; and
- Encouraging renewed attention to compliance activities.

Every covered entity – regardless of type or size – is eligible for an audit.

Audit Scope

Covered entities and Business Associates subject to OCR audits include:

Individual and Organizational Health Care Providers

Health Plans of All Types

Health Care Clearinghouses

Business Associates

Audit Protocol – 11 Modules

Compliance is evaluated and assessed based on established Privacy Rule, Security Rule and Breach Notification criteria, audit testing procedures, and applicability.

Privacy

- Notice of Privacy Practices
- Rights to Request Privacy
- Protection of PHI
- Access of Individuals to PHI
- Administrative Requirements
- Uses and Disclosures of PHI
- Amendment of PHI
- Accounting of Disclosures

Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Breach Notification

Pilot Audit Findings – Widespread Noncompliance

The initial wave of OCR audits of covered entities clearly identified privacy and security areas of noncompliance.[2]

For every finding and observation cited in the audit reports, the audit identified a "Cause." The most common across all entities: **entity unaware of the requirement**. Auditors found that even though Privacy, Security and Breach Notification Rules explicitly state what a covered entity must do to comply, elements were missing. They also discovered that some entities completely disregarded the requirements.

Does Any of This Describe Your Organization?

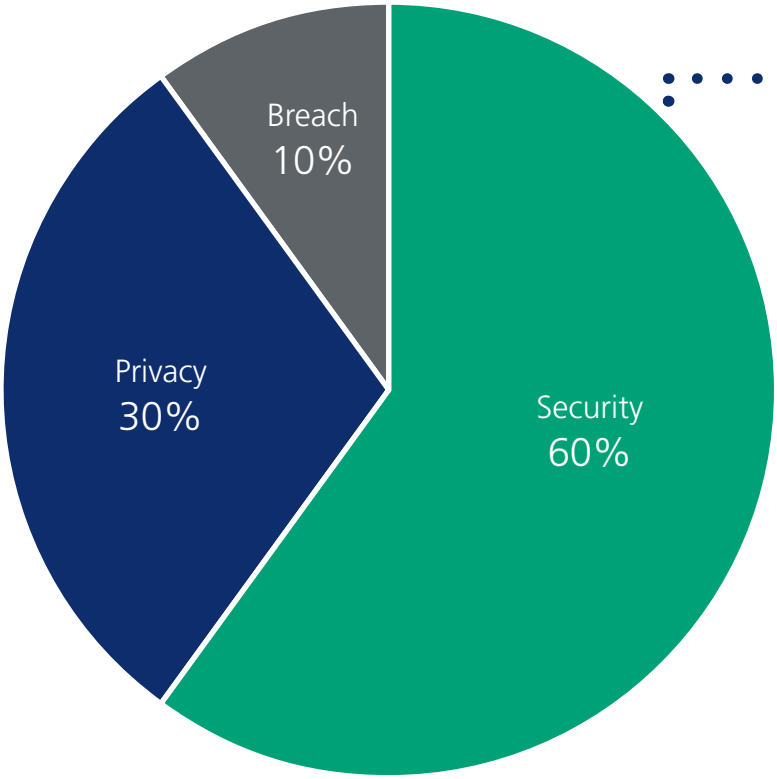
Common Privacy Areas of Noncompliance

- Notice of Privacy Practices
- Access of Individuals to PHI
- Minimum Necessary
- Authorizations

Common Security Areas of Noncompliance

- Risk Analysis
- Media Movement and Disposal
- Audit Controls and Monitoring

Proportional Findings and Observations by Rule



Notable Security Results

58 of **59** providers had at least one Security finding or observation

No complete and accurate risk assessment in **2/3** of entities

- **47** of **59** providers
- **20** of **35** health plans
- **2** of **7** clearinghouses

[a] Rinker. Source Data: U.S. Department of Health and Human Services, Office for Civil Rights.

REALITY CHECK 3

WORKFORCE MEMBERS POSE A SIGNIFICANT RISK FOR HIPAA LIABILITY

Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5). The U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities, business associates and individuals, who "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification regulations face fines, as well as imprisonment.

A tiered civil penalty structure for HIPAA violations is in place, and it's critical for employees to understand that they are personally subject to fines and criminal penalties.

Tiers of Civil Money Penalties for HIPAA/HITECH Violations

Penalties are measured for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation.

Violation Category	PENALTY, Each Violation	MAXIMUM PENALTY for Violations of an Identical Provision in a Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect - Not Corrected	$50,000	$1,500,000

The 2013 Final Omnibus Rule Strengthened the Government's Ability to Enforce the Law

OCR enforces the Privacy and Security Rule by:

- Investigating complaints filed with it; and
- Conducting compliance reviews to determine if covered entities are in compliance.

OCR refers possible criminal violations of HIPAA to the Department of Justice (DOJ). 42 U.S.C. § 1320d-6

Do All Workforce Members Understand HIPAA Violations May Be a Crime?

Federal law prohibits any individual from improperly obtaining or disclosing protected health information from a covered entity without authorization.

Violations may result in the following criminal penalties:[5]

Prohibited Conduct	Penalty
Knowingly obtaining or disclosing protected health information without authorization.	Up to $50,000 fine and **one year** in prison
If done under false pretenses.	Up to $100,000 fine and **five years** in prison
If done with intent to sell, transfer, or use the information for commercial advantage, personal gain or malicious harm.	Up to $250,000 fine and **ten years** in prison

More Than One in Three Data Breaches Are Caused by Workforce Members

HIPAA liability stemming from the actions of workforce members (including employees, volunteers, and trainees) is a bigger issue than you may realize. In 2013, Forrester Research conducted a survey of IT executives and found that employees having lost, stolen, or inadvertently misusing data, caused 36% of data breaches. The report also found that only 57% of employees said they were familiar with their company's security policies.[6]

Human Error and Malicious Intent Are Working Against You

An often overlooked cause of privacy breaches is human error. Workforce members with the best of intentions can still be careless or make mistakes. Health information may be mishandled and files may be disposed of improperly.

The experience of Kroll, an organization specializing in cyber security, sheds light on the prevalence of malicious intent. Examining data from cases Kroll handled for clients in 2013, it found that 78% of healthcare cyber crises were tied to human error, and 22% involved an act of malicious intent.[7]

Mistakes by employees can potentially be as damaging as actions of willful or malicious intent, as demonstrated in these cases investigated by OCR.[8]

Federal law prohibits any individual from improperly obtaining or disclosing protected health information from a covered entity without authorization.

Employee mistakenly emails PHI to other patients

An employee of a business associate mistakenly sent an email to multiple patients in which the names and email addresses of 937 individuals were visible to all recipients. OCR required retraining of employees on the requirements of Privacy and Security Rules, as well as on related policies and procedures.

Employees maliciously share PHI with a competing practice

Employees of a medical practice stole PHI pertaining to 13,000 patients and disclosed the information to a competing medical practice. The PHI included names and contact information. The entity terminated the employees. Even though the entity had complied with the Breach Notification Rule, OCR required it to retrain its workforce regarding the policies and procedures for safeguarding PHI.

REALITY CHECK

4 PATIENTS ARE AWARE OF THEIR RIGHTS TO FILE A COMPLAINT

The public is becoming increasingly concerned about their personal information. Frequent media reports about corporations and healthcare organizations that have compromised passwords, personal data or payment information have amplified a general concern about the safety of personal data, including PHI.

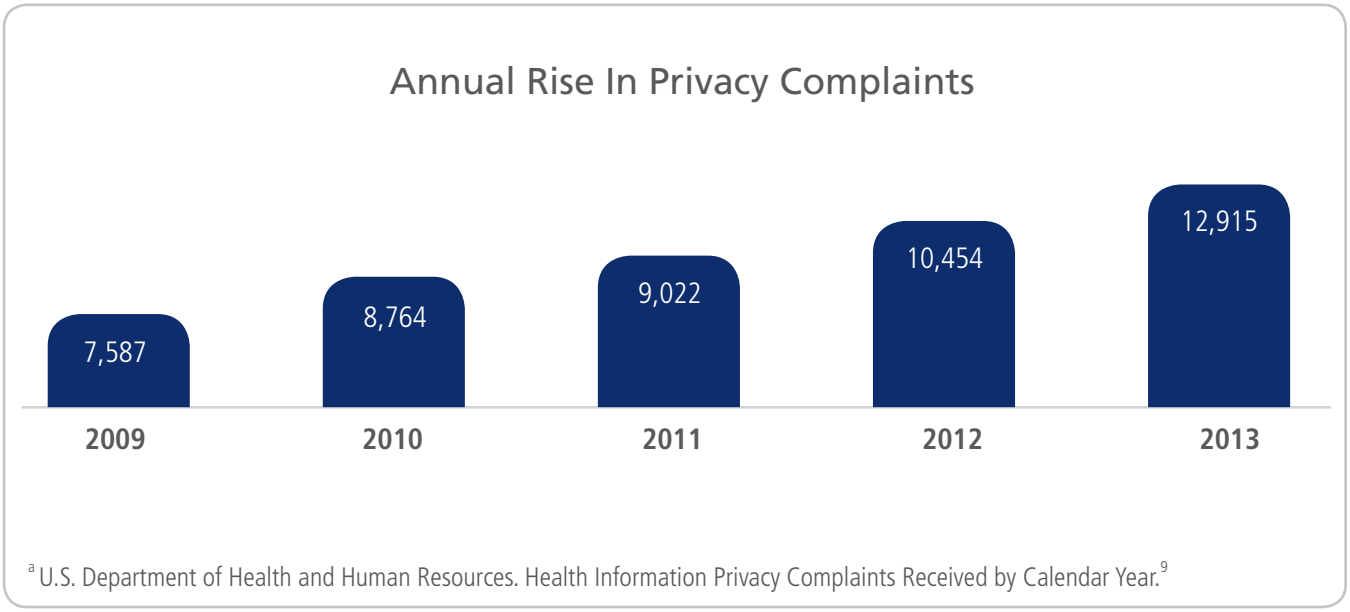
Ongoing reports of major breaches of PHI only serve to heighten awareness and concern in patients. Now more than ever, patients are beginning to understand their privacy rights and have greater expectations that their health information will be protected.

OCR Has Made It Easier to File a Complaint

In July 2013, OCR created a new web-based portal that makes it easier for patients to file a complaint involving a believed violation of health information privacy, security, and patient safety rules. Even a person who is not the patient can file a complaint on behalf of another.

The OCR complaint portal is part of a strategic approach to increase efficiencies involving the identification of cases to investigate. Once a complaint has been filed and reviewed, and where there is jurisdiction, OCR will investigate the alleged action or omission to determine if a violation or potential violation has occurred.

OCR Director Jocelyn Samuels reported at the 2015 National HIPAA Summit that HHS expects to receive 17,000 complaints in 2015.[3]



[a] U.S. Department of Health and Human Resources. Health Information Privacy Complaints Received by Calendar Year.[9]

Patient Rights Under HIPAA

Under HIPAA, with limited exceptions, a patient has a right to:

- Communicate confidentially;
- Access, view and receive copies of their medical/billing records; (within the Designated Record Set)
- Request an amendment/correction of their PHI;
- Restrict disclosures of PHI;
- Control the sale, marketing and research related uses of their PHI;
- Receive a Notice of Privacy Practices that outlines how their PHI will be used and disclosed;
- Request an accounting of who their health information has been disclosed to;
- Receive notice of a breach of their PHI; and
- File a complaint with OCR (Office for Civil Rights).

The OCR complaint portal receives approximately 200 complaints each week.

Covered entity providers must post and make available the Notice of Privacy Practices (NPP) for protected health information to provide a clear explanation of patient rights with respect to personal health information, including how to file a complaint.

Providers must amend their NPPs to reflect HIPAA Omnibus Final Rule changes, including those related to breach notification, disclosures to health plans, and marketing and sale of PHI.

REALITY CHECK

5 OCR IS INCREASING ITS FOCUS ON HIPAA ENFORCEMENT

Whether a covered entity's notice of a reportable breach or a complaint triggers investigation, OCR reviews the information or evidence that it gathers in each case. In some cases, it is determined that the covered entity did not violate the requirements of the Privacy or Security Rule. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining: 1) Voluntary compliance; 2) Corrective action; and/or 3) Resolution agreement.

OCR reported that in 2013 there were 4,459 investigative closures, with nearly 78% of those investigations having been closed with corrective action related to their enforcement.[10]

From 2008-2014, over $30 million in Resolution Agreements and fines have resulted.[11]

Covered Entity	Fine	Date
Anchorage Community Mental Health Services	$150,000	December 2, 2014
Parkview Health Systems Inc. (Parkview)	$800,000	June 23, 2014
New York Presbyterian Hospital (NYP)	$4,800,000	May 7, 2014
Concentra Health Services	$1,725,220	April 22, 2014
QCA Health Plan	$250,000	April 22, 2014
Skagit County, Washington	$215,000	March 7, 2014
Adult & Pediatric Dermatology, P.C. of Massachusetts	$150,000	December 20, 2013
Affinity Health Plan	$1,215,780	August 14, 2013
WellPoint	$1,700,000	July 11, 2013
Shasta Regional Medical Center	$275,000	June 13, 2013
Idaho State University	$400,000	May 21, 2013
Hospice of North Idaho	$50,000	December 31, 2012
Massachusetts Eye and Ear Institute	$1,500,000	September 17, 2012
Alaska DHSS	$1,700,000	June 26, 2012
Phoenix Cardiac Surgery	$100,000	April 13, 2012
BCBS Tennessee	$1,500,000	March 13, 2012
UCLA Health System	$865,500	July 6, 2011
Massachusetts General Hospital	$1,000,000	February 14, 2011
Cignet Health	$4,300,000	February 4, 2011
(Summary Judgment US District Court for Cignet)	$4,782,845	August 28, 2013
Management Services Organization of Washington	$35,000	December 13, 2010
Rite Aid Corporation	$1,000,000	July 27, 2010
CVS Pharmacy, Inc.	$2,250,000	January 16, 2009
Providence Health & Services	$100,000	July 16, 2008

Other Enforcement Actions

Even when OCR doesn't penalize the breached and investigated entity with a fine, OCR's enforcement may require actions to remedy the complaint and may issue directives for future compliance. Ongoing scrutiny by OCR and possibly other governmental agencies, such as the Federal Trade Commission (FTC), may be involved.

The Risk is Real

Here are a few examples:[8]

Dentist Revises Process to Safeguard Medical Alert PHI
An OCR investigation confirmed allegations that a dental practice had flagged some of its medical records with a red sticker containing the acronym "AIDS" on the outside cover. Records were also handled in a manner that allowed other patients and staff (without the need to know) to read the sticker. Even though the practice removed the stickers when notified of the complaint, OCR directed the practice to make significant changes in its policies and procedures and to move medical alert stickers to the inside cover of the records.

Clinic Sanctions Supervisor For Accessing Employee Medical Record
After investigating a supervisor's access, examination, and disclosure of an employee's medical record, OCR concluded the use and disclosure were not authorized by the employee and were not otherwise permitted by the Privacy Rule. Because an employee's medical record is protected, OCR directed the clinic to reprimand the supervisor and provide training about the Privacy Rule, and counseling about the appropriate use of the medical information of a subordinate.

Outpatient Facility Corrects Privacy Procedure
An outpatient surgical facility mistakenly disclosed a patient's protected health information to a research entity for recruitment purposes without the patient's authorization, or an Institutional Review Board or privacy-board-approved waiver of authorization. OCR required the outpatient facility to revise its written policies and procedures, retrain its entire staff on the new policies and procedures, log the disclosure of the patient's PHI for accounting purposes, and send the patient a letter apologizing for the impermissible disclosure.

No entity that manages PHI is beyond the reach of OCR or numerous government agencies that may claim jurisdiction for enforcement actions of health information violations. Criminal liability for HIPAA violation enforcement actions can be initiated by the U.S. Department of Justice. State statutes, unless preempted by HIPAA, may also impose both criminal sanctions and civil penalties.

REALITY CHECK

6 HIPAA COMPLIANCE IS NOT AN OPTION, IT'S LAW

HIPAA is a complex set of rules, and it's Administrative Simplification regulations are being enforced with greater intensity. But you don't have to become an expert in privacy, security and breach notification laws and requirements to stay in compliance. What you need is help to implement the required controls, workforce education, proper documentation, and continual risk analysis and monitoring that will mitigate the risk of stiff financial penalties, lawsuits, and damage to your reputation.

Noncompliance is Expensive

Fines can range from thousands to millions of dollars. Making an upfront investment of time and resources to become and stay compliant is a better business decision than paying the costs to recover from a breach or violation. Worse, these costs can be financially crippling to a practice.

Noncompliance Drives Away Patients

Fines and enforced corrective action are a financial burden, but you also risk losing your business or damaging your brand. According to the 2013 Survey on Medical Identity Theft conducted by the Ponemon Institute, 57% of consumers would switch health care providers, if they knew their provider could not safeguard their medical records. They simply lose trust and confidence in their health care provider.

It's Up to You

In order to be in compliance, practice owners and office managers must demand a culture of compliance. You can proactively mitigate risk by fully implementing a compliance program that meets HIPAA requirements for workforce education, proper documentation, and continual risk analysis and monitoring.

Smaller organizations — even those with the most conscientious providers — are increasingly turning to third-party providers to help with identifying risks and security threats, training staff, documenting policies, and assisting with ongoing compliance.

57% *of consumers would switch health care providers, if they knew their provider could not safeguard their medical records.*[4]

BE PROACTIVE AND GET THE HELP YOU NEED TO COMPLY

HIPAA privacy and security compliance rules are changing. Enforcement is intensifying. The risk of breach is rising. Public concern is increasing.

The reality is that the cost of a single breach could devastate your practice, your reputation, and your priceless brand in your community.

No covered entity organization is too big — or too small — to escape the regulators or civil lawsuits. You must act proactively to reduce your risk by focusing your internal team on compliance activities, or by engaging a qualified third-party provider to evaluate your risk and provide the ongoing support and resources you need to feel confident in your organization's ongoing compliance.

Steri•Safe℠ HIPAA Compliance Solutions by Stericycle is a comprehensive program that can help you eliminate confusion over the extensive Omnibus revisions and address the risks and costs of "doing nothing."

By easing your compliance burdens, Steri•Safe℠ HIPAA Compliance Solutions help you focus on patient care.

BE STERI•SAFE℠

Protect Your Business With the Best

Navigating the complex demands of HIPAA compliance is daunting. As a leader in compliance solutions, we guide you through the maze.

Convenient and User-Friendly Compliance

With Steri•Safe℠ HIPAA Compliance Solutions, we help ensure your facility is protected.

Our Steri•Safe℠ HIPAA Compliance Solutions include:

- Risk Assessments (Privacy & Security)
- Online and/or On-Site Training
- Policy Documentation Resources

STERI•SAFE℠
COMPLIANCE SOLUTIONS

For more information, visit www.Stericycle.com/HIPAA or call 866-783-9814

REFERENCES

1. Citation: (Johnson and Goetz 2007). Ajit Appari, M. Eric Johnson, Denise L. Anthony, *HIPAA Compliance: An Institutional Theory Perspective. (2009)*. Downloaded from http://www.ists.dartmouth.edu/library/489.pdf

2. Verne Rinker JD, MPH. *HIPAA Privacy, Security and Breach Notification Audits*. Program Overview & Initial Analysis presented at 2013 NIST/OCR Security Rule Conference, May 21-22 2013. Downloaded from http://csrc.nist.gov/news_events/hipaa-2013/presentations/day1/rinker_day1_215_hipaa_privacy_security_breach_audits.pdf

3. Jocelyn Samuels, Director, HHS Office for Civil Rights. Keynote Address. Presented at 23rd National HIPAA Summit, March 16, 2015.

4. Ponemon Institute Research Report. *2013 Survey on Medical Identity Theft*. Publication Date: September 2013. Research sponsored by the Medical Identity Fraud Alliance with support from ID Experts.

5. Kim Stanger. Holland & Hart News Update. April 25, 2012. Downloaded from http://www.hollandhart.com/pubs/uniEntity.aspx?xpST=PubDetail&pub=1898

6. Heidi Shay. *Understand the State of Data Security and Privacy*: 2013 to 2014. Forrester Research Inc. Oct. 1, 2013 http://www.mobility-sp.com/images/gallery/FORRESTER-Understand-The-State-Of-Data-Security-And-Privacy-2013-To-2014.pdf

7. Kroll Special Report: *Healthcare, Higher Education, Finance Industry Clients Top Three Cyber Targets in 2013*. Published 2014.

8. U.S. Department of Health and Human Resources. Case Examples Organized by Covered Entity: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/casebyentity.html

9. U.S. Department of Health and Human Resources. Health Information Privacy Complaints Received by Calendar Year: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html

10. Susan McAndrew, JD, Deputy Director, Health Information Privacy Division. *OCR Update and Outreach, Stepping Up Compliance in 2014*. Presented at 22nd National HIPAA Summit, February 5, 2014.

11. U.S. Department of Health and Human Resources. Case Examples and Resolution Agreements: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

www.Stericycle.com/HIPAA

866-783-9814

Stericycle®

28161 N. Keith Drive
Lake Forest, IL 60045

Copyright © 2015 Stericycle, Inc. All rights reserved.