

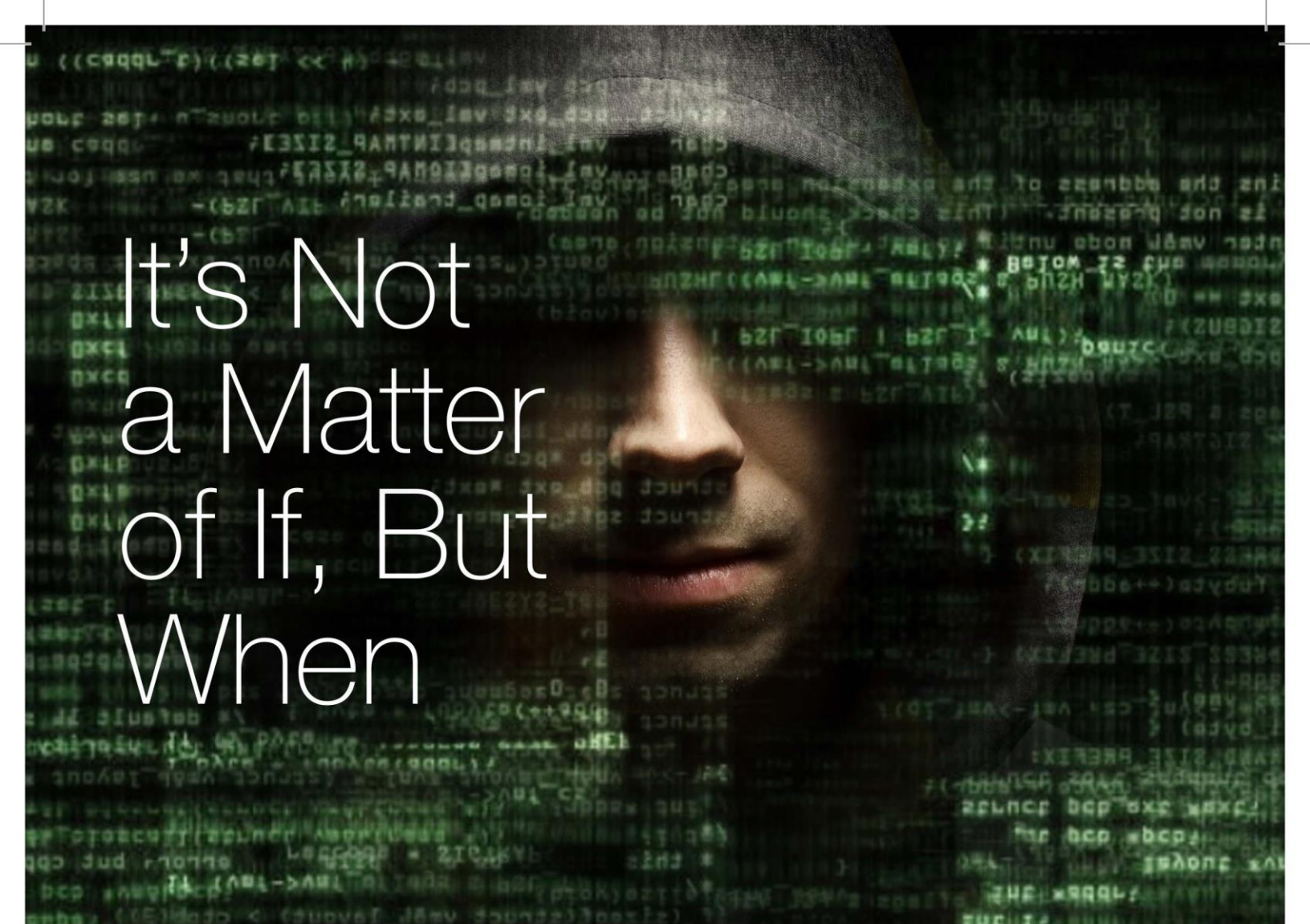


HIPAA Security Compliance

10 RED FLAGS



Copyright © 2016 by CAEK, Inc. All rights reserved. Private and Confidential.

A person wearing a dark hoodie is shown from the chest up, looking slightly to the right. The background is a dark, textured surface with green and white digital code or binary data floating around, creating a high-tech, cybernetic atmosphere.

It's Not a Matter of If, But When

HIPAA Security breaches like **stolen laptops**, **patient complaints**, and **computer viruses** happen every day to practices just like yours.

Do you have the critical parts of HIPAA security compliance to survive a HIPAA incident?

LAYERCOMPLIANCE™ can help!

LayerCompliance™ is the **online HIPAA security compliance program** that can help you get in and stay in compliance.

Visit
LayerCompliance.com
today to learn more and
take **our free compliance
assessment** to see if you are
truly prepared.

1-800-334-6071

RISK ANALYSIS

#1 Missing Threat Analysis

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, “[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”

As provided in the guidance from the Office for Civil Rights (OCR)¹ and the National Institute of Standards and Technology (NIST)², covered entities need to assess potential risks based on threats, for example:

- Natural threats: floods, tornadoes, earthquakes, tornados, and landslides
- Human threats: are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- Environmental threats: may include power failures, pollution, chemicals, and liquid leakage.

Your risk analysis should identify the likelihood, impact, and risk for specific threats, such as lost or stolen devices, computer virus (malware), and malicious insider, as well as natural and environmental threats.

#2 Safeguards Not Identified for Specific Threats

In addition to documenting your organization’s threats, your risk analysis should also document the safeguards that can reduce risk to a reasonable and appropriate level, as well as comply with the standards and implementation specifications in the HIPAA Security Rule.

*Once risk is identified and assigned a risk level, the covered entity should begin to **identify the actions required to manage the risk**. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization’s policies and procedures.³*

¹ Department of Health & Human Services: *HIPAA Security Series: 6 Risk Analysis and Management*
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>

² National Institute of Standards and Technology (NIST) Publication 800-30 *Guide for Conducting Risk Assessments*
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

³ Department of Health & Human Services: *HIPAA Security Series: 6 Risk Analysis and Management*
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>

Your risk analysis should identify the specific safeguards to reduce risks of threats, such as encryption for a lost/stolen device, or maintaining software with the latest security patches for malware (computer virus).

POLICIES AND PROCEDURES

#3 Do Not Have HIPAA Security Policies

Many covered entity assume that they have HIPAA policies, without understanding the difference between HIPAA Privacy policies and HIPAA Security policies. HIPAA Privacy policies include appropriate disclosure and authorization for disclosure of patient information, providing patients with your notice of privacy, etc. You must also have written policies for each of the standards and implementation specifications in the HIPAA Security Rule, such as policies for encrypting devices, preventing malicious software, securing your facility, etc.

You should have policies and procedures that cover the 18 standards and 36 implementation specifications in the HIPAA Security Rule, such as Encryption, Protection from Malicious Software, Log-in Monitoring, etc.

#4 Guides, Templates, and Toolkits Not Completed

Did you buy a policy manual and stick it up on your shelf? Are your policies “customized” with your practice name and address? Your written policies must be accurate and you must be able to document that you are following your written policies. Review your HIPAA security policies and see if they are complete and if your practice has implemented what is written. In most cases, template policies require several weeks of your HIPAA Security Officer’s time to review, modify, and adopt written policies that fit your practice.

Covered entities have been fined for using template policies that were not followed.⁴

⁴ Department of Health & Human Services Bulletin *HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software* <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf>

#5 Missing Documents Referenced in Policies

Many policy templates and purchased manuals have policies that refer to other documents that you are responsible for creating and maintaining. For instance, part of your Security Management Process: Risk Management policy likely states that you will have a written Risk Management Plan. Your Contingency Plan policy may require a Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.

If you have not created all of the documents referenced in your policies, such as a Risk Management Plan, you may not be complying with your own written policies and may be at risk for higher “willful neglect” HIPAA penalties.

#6 No Policies for Addressable Implementation Standards

When policy templates and guides are purchased, the policies for the “addressable” implementation standards often require the practice to review the policy and determine if it is reasonable to implement as written or if the practice needs to put an alternate policy in place. If you don’t document how these addressable policies will be implemented, you may not have a written policy in place for that requirement. Review your policies for the addressable implementation specifications, such as Termination Procedures, Log-in Monitoring, Password Management, Encryption and Decryption, etc.

If your policy templates require you to analyze “addressable” policies, you may not have a policy in place if you have not documented what is reasonable for your practice. Addressable does not mean optional.

IMPLEMENTATION

#7 Missing Implementation Plan

A risk analysis is not enough. You need to have a written plan for implementing the safeguards that are appropriate for your practice. Performing a risk analysis without an implementation plan is like going to a mechanic, placing the list of problems found into your glove box, and then driving your car home with no plans to fix anything. Even if you can’t pay for everything your mechanic recommends immediately, you need to have a plan to fix the major issues.

Identifying a threat in your risk analysis without a plan to implement safeguards to mitigate the risk can lead to heavy fines – you must have an Implementation Plan.⁵

#8 No Documentation of HIPAA Activities

Like any other federal regulation, you must keep a record of your compliance, including the implementation of the safeguards to comply with the HIPAA Security Rule and mitigate your risk.

If it isn't documented, it didn't happen. Record dates, personnel who performed or verified, and other applicable details when safeguards are implemented.

MONITORING AND AUDITING (RISK MANAGEMENT)

#9 Ongoing Compliance Not Reviewed

The HIPAA Security Rule requires you to verify your compliance on an ongoing basis. 45 CFR § 164.306(e) (a)(4) states:

"[(Covered entities and business associates must do the following)] [e]nsure compliance with this subpart [(the Security Rule)] by its workforce" 45 CFR 164.306(a)(4)

You need documentation of ongoing compliance, such as when software is updated with the latest security patch, review of audit logs, verifying termination procedures were followed, etc.

⁵ Department of Health & Human Services Press Release *Stolen laptops lead to important HIPAA settlements*
<http://www.hhs.gov/news/press/2014pres/04/20140422b.html>

#10 New Technology or Operations Not Evaluated

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

“Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 [(the Organizational Requirements)] and this subpart [(the Security Rule)] must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of [EPHI] as described at § 164.316.”

The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

“Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [EPHI], that establishes the extent to which an entity’s security policies and procedures meet the requirements of [the Security Rule].”

You need to assess new technology or operations, such as upgrading your EHR for Stage 2 Meaningful Use or beginning a social media program for your practice, and implement the appropriate safeguards to comply with the HIPAA Security Rule.

WHAT HAPPENS IF YOU AREN'T IN COMPLIANCE?

Failing to comply with HIPAA has far reaching consequences, and a patient complaint, HIPAA incident, or breach report can prompt an investigation by the Office for Civil Rights (OCR).

\$150,000 HIPAA Fine⁶

“...adopted sample Security Rule policies and procedures...”

“...the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software”

⁶ Department of Health & Human Services Bulletin *HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software* <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf>

\$50,000 HIPAA Fine⁷

"...had not conducted a risk analysis... did not have policies or procedures to address mobile device security"

\$1,975,220 Fine⁸

*"...previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. **While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time**"*

Breach Costs per Record \$398 in 2015⁹

"The cost of data breach sets new record high"

Cyber Liability Insurance Claim Denied¹⁰

"Insurer cites cyber policy exclusion to dispute data breach settlement... failure to follow minimum required practices"

Lose 54% of Your Patients¹¹

"54% very likely or likely to change providers following a data breach"

\$1.44 Million Dollar Verdict Against Walgreens¹²

"Indiana Court of Appeals upheld a \$1.4 million verdict against Walgreens Co. and one of its pharmacists who shared confidential medical information about a client that had once dated her husband"

⁷ Department of Health & Human Services Press Release *Hospice of North Idaho settles HIPAA security case for \$50,000*
<http://www.hhs.gov/news/press/2013pres/01/20130102a.html>

⁸ Department of Health & Human Services Press Release *Stolen laptops lead to important HIPAA settlements*
<http://www.hhs.gov/news/press/2014pres/04/20140422b.html>

⁹ Ponemon Institute Research Report, *2015 Cost of Data Breach Study: United States*

¹⁰ U.S. District Court in Los Angeles *Casualty Co. v. Cottage Health System*

¹¹ Software Advice, Austin, TX *Data Breach Patient Survey 2015*

¹² Indy Star <http://www.indystar.com/story/news/2014/11/14/m-award-upheld-walgreen-pharmacist-shared-patient-data/19035783/>

LAYERCOMPLIANCE™— A COMPREHENSIVE PROGRAM

CONSULT-LEVEL SERVICE. COST EFFECTIVE PRICE.

Risk Analysis

A full Risk Analysis that assesses systems and provides both HIPAA Security compliance and threat analysis.



Policies & Procedures

Custom HIPAA Security policies based on your individual organization—not generic templates.

Implementation

You can document HIPAA Security compliance activities, including the implementation of policies and security measures.



Risk Management

A once-a-year audit or assessment isn't enough. Breaches can happen every day and you need to stay in compliance all year round.

With LayerCompliance™, organizations can get the expert help and tools they need to get in and stay in compliance.



Live Support

Our team is ready to assist with HIPAA Security questions, incidents and potential breaches



HIPAA Security Training

We provide HIPAA Security awareness & security policy staff training

LAYERCOMPLIANCE™

800.334.6071