



Suze Shaffer, CHSP



Suze is a Certified Healthcare Security Professional and the president of Aris Medical Solutions since 2009.

Suze has been instrumental in helping hundreds of clients nationwide with risk management and protecting patient data.

Suze and her team stand between you and the government regulations, ensuring you understand what is required and how to accomplish the task.

Most important, how to meet the requirements and avoid fines and penalties!



Who are we? What do we do?



- Annual HIPAA Risk Analysis
- HIPAA training (customized)
- Breach notification plan
- Security incident / breach forms
- Patient privacy policies
- Patient request forms
- Security policies and procedures
- Security documentation forms
- Contingency plans
- Consulting and implementation

The image is a composite graphic. The top portion shows a close-up of a silver stethoscope resting on a white surface, with a blurred medical chart in the background. The bottom portion features a pair of glasses with a white frame and a silver stethoscope resting on a medical chart. The chart has several colorful tabs (green, blue, orange, red) with numbers and letters like '3', '1', '8', '3', '5', '3', '7', '5', '3', '4', '6', 'M'. The text 'HIPAA Compliance Officer Training' is overlaid in white on a black background on the right side of the image.

HIPAA Compliance Officer Training



Webinar Topics

- What is HIPAA and its history (summary)
- Who is required to adhere to HIPAA
- Understanding some of the Privacy Rule requirements to guide your staff
- Understanding the Security Rule requirements for the Compliance officer
- How the Enforcement Rule can affect your organization
- What are Recognized Security Practices (RSPs)
- How to adhere to the Information Blocking Rule

A stethoscope and a pen are resting on a desk. In the background, a calendar is visible with various dates and colors. The word "Poll" is written in a large, blue, sans-serif font in the upper right corner of the slide.

Poll

I would like to know my audience to better gauge this training, what would best describe your duties?

- a. Privacy Officer
- b. Security Officer
- c. Both, Privacy and Security Officer
- d. Administrator that oversees the Compliance Officer(s)



HIPAA Privacy & Security Rules

HIPAA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA was enacted by the United States Congress and signed into law in **1996**. It set the standards for implementing provider and payer identification numbers.

Privacy Rule, 2003 was enacted to regulate the use and disclosure of protected health information (PHI).

Security Rule, 2005 was introduced to outline the requirements needed to secure electronic data against threats and vulnerabilities.



Enforcement, HITECH Act, & Omnibus Rules



Enforcement Rule, 2006 contains provisions relating to compliance and investigations, the implementation of civil money penalties for violations, and procedures for hearings.

HITECH Act, 2009 was enacted as part of American Recovery and Reinvestment Act (ARRA) to promote the adoption and meaningful use of Electronic Health Records (EHR).

Omnibus Rule, 2013 known as the Final Rule, strengthened the Enforcement Rule and updated the HIPAA Security and Breach Notification Rule.



Enforcement Results

From the compliance date to the present, the compliance issues most often alleged in complaints are in order of frequency:

- Impermissible uses and disclosures of protected health information (hacking and unauthorized access);
- Lack of safeguards of protected health information (physical and technical);
- Lack of patient access to their protected health information;
- Lack of administrative safeguards of electronic protected health information (policies and procedures); and
- Use or disclosure of more than the minimum necessary rule for protected health information.

This was taken straight from the OCR's website.



Who must adhere to HIPAA?



Under the HIPAA Rules...
Covered Entities, Business
Associates, and
Subcontractors of Business
Associates must follow the
HIPAA Rules and are subject
to fines and penalties for
violations.



Who are Covered Entities?

Health Care Providers: Doctors, Dentists, Chiropractors, Clinics, Nursing Homes, Pharmacies.

Health Plans: Health insurance companies, Company health plans, HMOs, Government programs such as Medicare, Medicaid, and the military and veterans' healthcare programs.

Health Care Clearinghouse: Entities that process nonstandard health information they receive into a standard format for the purpose of processing information for payments



What is a Business Associate?

A Business Associate (BA) is a person or entity that performs services that involve the use or disclosure of protected health information (PHI) for a covered entity.

A member of the covered entity's workforce is not a business associate nor is a cleaning company.



Who are Business Associates?

- *Answering services*
- *Attorneys*
- *Billing companies*
- *Biomedical equipment maintenance & repair services*
- *Clearinghouses**
- *Collection agencies (if they receive more than basic demographics)*
- *Copier / equipment leasing company***
- *CPA*
- *Electronic health/medical records software*
- *Insurance verification software*
- *IT professionals or consultants*
- *Payment software (if used in conjunction with claims being adjudicated)*
- *Practice management software*
- *Record storage companies*
- *Shredding companies*
- *Telemedicine vendors*
- *Transcription services*
- *X-ray destruction companies*

** Clearinghouses can be a Covered Entity or a Business Associate of a Covered Entity.*

*** If they service the equipment or equipment is returned to them.*



Doing business with a BA



A Covered Entity may only permit a BA to create, receive, maintain, or transmit ePHI if they obtain satisfactory assurances that the BA will appropriately safeguard protected health information.

This includes obtaining a Business Associate Agreement (BAA) and other documentation that demonstrates their compliance efforts, such as a risk analysis, HIPAA training certificates, and HIPAA policies and procedures.

Covered entities also have the right to ask their BA if they use Subcontractors and obtain a copy of that BAA.



Why are BAAs important?

Raleigh Orthopedic was fined **\$750K** for releasing X-Rays films to a company that didn't destroy the films in a HIPAA compliant manner.

Athens Orthopedic Clinic was fined **\$1.5M** for multiple violations including the lack of a BA agreement that led to a breach.

Cottage Health was fined **\$3M** after their IT vendor misconfigured a Windows Operating system that shared PHI on the internet.

Touchstone Medical Imaging was fined **\$3M** after the FBI discovered that one of their FTP servers allowed uncontrolled access to patient information on the internet.

If these practices had a BA agreement in place, these fines could have been placed on the Business Associate instead.



Privacy Officer Duties



The **Privacy Rule** requires that all Covered Entities (CEs) assign someone who is responsible for the creation, implementation, and enforcement of the Privacy Rule. This is referred to as the Privacy Officer.

The **Privacy Officer** oversees patient rights and patient documentation.



Security Officer Duties



The **Security Rule** requires that all Covered Entities (CEs) and Business Associates (BAs) assign someone who will be responsible for the creation, implementation, and enforcement of the Security Rule. This is known as the Security Officer.

The **Security Officer** oversees the electronic data and the physical and technical safeguards of ePHI.



HIPAA Compliance Officer

laws **RULES**
regulations
PROCESS consistency
COMPLIANCE
GUIDELINES security STANDARDS
policy MANAGING RISK
mitigation adherence **PROTECT**
ENFORCE audit
adherence **SAFETY**

The responsibility of Privacy and Security can be assigned to one person and referred to as the “**HIPAA Compliance Officer**”.

EVERYONE MUST KNOW WHO THEIR COMPLIANCE OFFICERS ARE!

It is recommended to place a 3”x5” card near each phone and the front desk reception area.



Compliance Documentation

All workforce members are required to adhere to the Policies and Procedures the officers have put in place, including management and physicians.

The officer(s) are required to document violations.

Remember, these titles are not to be taken lightly, they come with state and federal requirements.



**COMPLIANCE
OFFICER**



What is the Privacy Rule?

The **Privacy Rule** addresses the use and disclosure of health information and an individual's privacy rights to control how their health information is used.

The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate.



What is PHI/ePHI?

Protected Health Information (PHI)

Which is “individually identifiable health information” transmitted or maintained in any form or medium (including orally or written).

Electronic Protected Health Information (ePHI)

Is “individually identifiable health information” created, transmitted, or maintained in an electronic form.

PHI/ePHI is any information about health status, whether past, present, or future, provision of health care, or payment for health care that can be linked to a specific individual.



What is considered PHI/ePHI?

- Names
- All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and [t]he initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- Dates (other than year) directly related to an individual
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers

- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Social media accounts
- **Any other unique identifying number, characteristic, or code** except the unique code assigned by the investigator to code the data.

Where is PHI?



Protected health information can be found in a variety of places such as:

- paper charts
- insurance cards
- office boards
- telephone notes
- dictation tapes
- fax machines
- copy machines
- delivery tickets

Where can ePHI be located?



- Electronic Health Records (EHR)
- Practice Management (PM)
- Copier/printer hard drives
- Scanners
- Email
- Spreadsheets
- Servers
- Workstations
- Laptops
- Tablets
- Smart phones
- Websites



What does Minimum Necessary mean?

The “Minimum Necessary” Standard requires that Covered Entities and Business Associates make all reasonable efforts not to use or disclose more PHI than is necessary to accomplish the intended function. This means only discuss a patient’s information with those that are involved with their treatment, payment for their care, health care operations, or is authorized by the patient.

The “Minimum Necessary” Standard requires organizations to limit unnecessary or inappropriate access and disclosure of PHI. This means that only people who need access to PHI to do their job should have access to this information.

“Minimum Necessary” means only supplying what is requested. Nothing more.



What about Snooping...



What if you discover a staff member accessing health records of patients for reasons other than for treatment, payment, and/or health care operations?

Snooping in healthcare records of family, friends, neighbors, co-workers, and celebrities is one of the most common HIPAA violations committed by employees.

This is a violation of patient privacy!

These violations usually result in termination. If the employee is not terminated, the organization could face charges and heavy fines.



Social Media



Patients commonly “check in” on Facebook or write about their experiences on Google. The Social Media person may respond with a thank you, but do not mention any services or diagnoses.

If it is a complaint, you may request they call the office to discuss the situation. Do not post anything about services provided or retaliate over what was said.



Social Media and Employees



Remind employees...

Do not post pictures or make comments about patients on business or personal social media sites!



There have been several fines assessed over inappropriate social media posts!



Notice of Privacy Practices

HIPAA PRIVACY FORM 1

Notice of Privacy Practices

Purpose: This form, Notice of Privacy Practices, presents the information that federal law requires us to give our patients regarding our privacy practices. (Note: this form may need to be changed to reflect the dental practice's particular privacy policies and/or stricter state laws.)

We must provide this Notice to each patient beginning no later than the date of our first service delivery to the patient, including service delivered electronically, after April 14, 2003. We must make a good-faith attempt to obtain written acknowledgement of receipt of the Notice from the patient. We must also have the Notice available at the office for patients to request to take with them. We must post the Notice in our office in a clear and prominent location where it is reasonable to expect any patients seeking service from us to be able to read the Notice. Whenever the Notice is revised, we must make the Notice available upon request on or after the effective date of the revision in a manner consistent with the above instructions. Thereafter, we must distribute the Notice to each new patient at the time of service delivery and to any person requesting a Notice. We must also post the revised Notice in our office as discussed above.

Patients have the right to receive a copy of how their information is collected, shared, and protected. This is called the Notice of Privacy Practices (NPP) and must contain an effective/revised date. If the practice participates in a Health Information Exchange (HIE) this must also be included in the NPP.

The notice must be posted in a location where patients are able to see it, and a copy must be provided to anyone who asks for one. It also needs to be prominently posted on any web site that provides information about services or benefits.



What does Right of Access mean?

Patients and their personal representatives have the “right of access” to protected health information (PHI), upon request in one or more "designated record sets".

This includes the right to inspect or obtain a copy, or both, as well as to transmit a copy to a person or entity of the individual's choice.

Although a written request is best, HIPAA prohibits undue restrictions when a patient makes this request.

However, you must make a “reasonable” effort to verify their identity. For example, if they are unable to come in the office to sign the request or they do not use email, a verbal authorization is permitted.



Right of Access time limit



HIPAA requires that you must answer the patient request within 30 days (15 days in the proposed rule), with one 30-day extension (15 days in the proposed rule). If you use an extension, you must advise the patient the reason for the delay and a date that their records will be made available. State laws that requires that access in a shorter time-period must be granted.

NOTE: Under Information Blocking, you must respond immediately or within a reasonable time frame.



Right of Access – how?

- Email is acceptable if you have explained this method is not secure and the patient still requests their PHI. Be sure to document the email acceptance. Then, delete the PHI email in a compliant manner or encrypt the data at rest.
- Patients have the right to view their records and may take pictures or notes.
- They also have the right to record office visits without your permission in all states *except* California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, New Hampshire, Nevada, Pennsylvania, and Washington. Since both parties must consent to being recorded. More states could be added at a later date.

It is recommended to take precautions in the event the patient does not disclose they are recording.

What exactly can we release?



The **Designated Record Set** is sometimes called the **DRS** – this is a group of records maintained by or for the medical practice. This includes the medical and billing records that are used in whole or part by the practice to make decisions about the individual.

Any medical information received from other medical providers may be included if this information is used to determine treatment for the patient.

Medical records retention



HIPAA does not dictate Medical Record Retention time requirements.

It is determined by state law.

Good Faith Estimate



A provider or facility must provide a good faith estimate of expected charges for items and services to an uninsured or self-pay individual.

The good faith estimate must include expected charges for items or services for the provider and/or facility including items or services that may be provided by other providers and facilities.

Organizations should post a notice to advise patients within their facility and on their website.



No Surprise Billing Act



No Surprises Act applies to items and services provided to most individuals enrolled in private or commercial health coverage. Some requirements also apply to providers and facilities with respect to uninsured or self-pay individuals.

Some health insurance coverage programs already have protections against surprise medical bills such as: Medicare, Medicaid, TRICARE, the Indian Health Services, and Veterans Health Administration. These programs have other protections against high medical bills.



Unauthorized disclosures

You must record in the patient's record whenever PHI is disclosed for anything other than for TPO. The note should include what was sent, (medical record, profile etc.) who it was sent to, and the date it was disclosed.

Patients have the right to request to see where, what, and to whom their PHI has been disclosed for the last six years from the date of request. This must be provided within 30 days.

This is called **"Accounting of Disclosures"** and includes:

- Misdirected fax, email, or mail.
- Release based on an invalid authorization.
- Public health authorities, as required by law, health oversight activities, and workers compensation are some examples.



What is the Security Rule?

NIST Special Publication 800-66 Revision 1



An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg

NIST, the National Institute of Standards and Technology created **The Security Rule in 2005.**

INFORMATION SECURITY

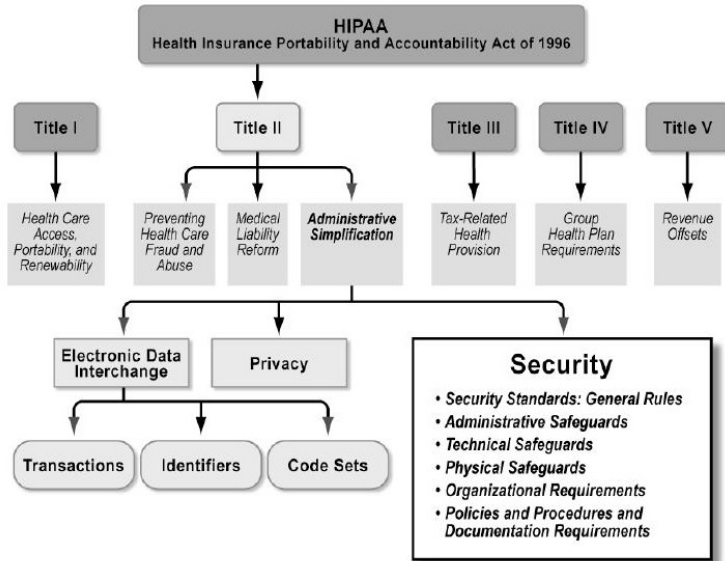


Figure 1. HIPAA Components

CBS_01527a

This rule was implemented to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

The HIPAA Security Rule



Security Standards Matrix (Appendix A of the Security Rule)

ADMINISTRATIVE SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

ORGANIZATIONAL REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)

HIPAA Risk Analysis



The lack of a system-wide risk analysis is the most common noted in resolution agreements from the OCR after an investigation.

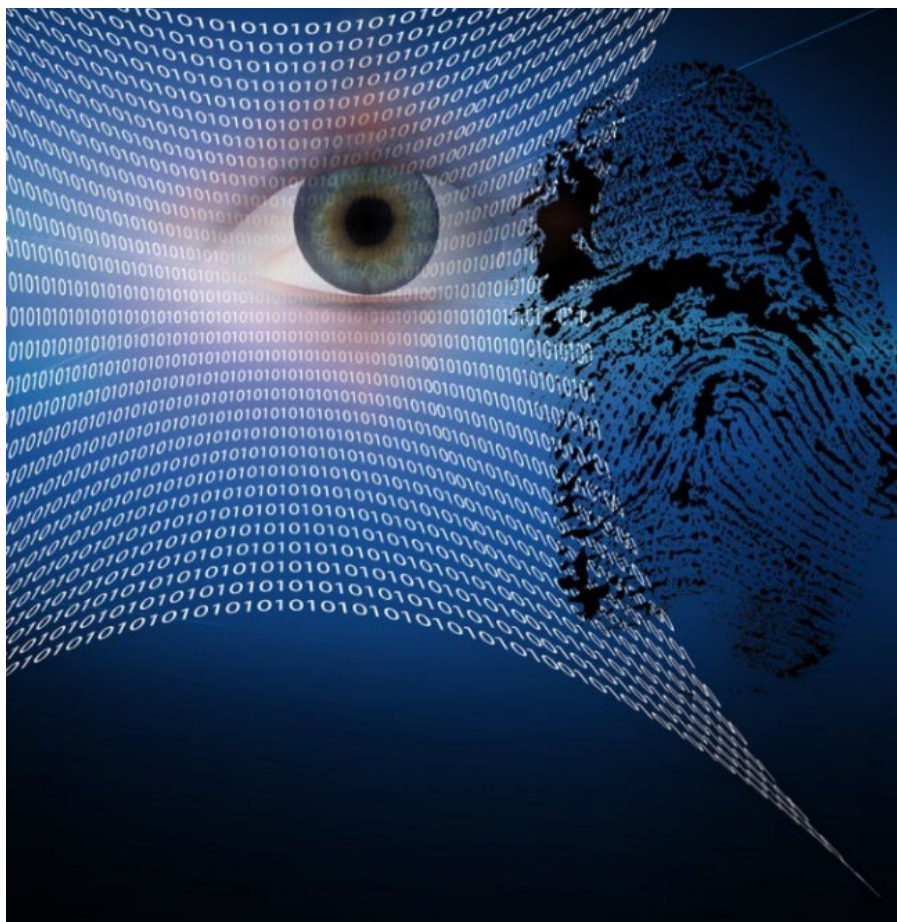
If your practice participates in MIPS, then most practices conduct their annual risk analysis during the last quarter of the year. Then prepare how to correct any deficiencies during the following year.

Other practices typically start their risk analysis in the first quarter of the year.

This is usually documented in a Risk Management Plan.



Information System Activity Review



The Security Rule requires any system that accesses or stores ePHI to be monitored for unauthorized access or activity.

Once an organization determines WHERE their ePHI is located, they must review the access and/or audit logs.

The HIPAA Compliance officer is responsible for this documentation, even though their IT department or outside vendor supplies this service.



Tiered Sanction Policy

Administrative Safeguards:		
Sanction Policy	§164.308(a)(1)(ii)(C)	Policy & Procedure: AS01.C
(R) Required		

HIPAA Security Standard:
"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

This policy applies to all workforce members

1. Purpose:
 Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with Security Policies and Procedures, and to deter noncompliance.

2. Policy:
 It is the policy of...
 HITECH...
 State laws, and the...
 to protect patient...
 use the form...
 d this document

NOTICE OF TERMINATION

Any member of the organization can be reprimanded in different ways including **termination**.

A person or company who deliberately releases PHI can face criminal and/or civil charges. They can be fined and/or receive up to 10 years in jail.

The 2014 Walgreens case, \$1.4M was awarded to Abigail Hinchy when a pharmacist violated a patient's privacy.



Security Awareness Training



HIPAA requires any individual that works with PHI to be properly trained in the Privacy, Security, and Breach notification rules.

Although HIPAA doesn't state a specific time frame when a new hire should be trained, it is recommended they be trained before given access to PHI or as soon as possible.

Annual HIPAA training is also recommended.



Security incidents

```
3 require File.expand_path("../config/application.rb", __FILE__)
4 # Prevent database truncation if the environment is production
5 abort("The Rails environment is running in production mode!")
6 require 'spec_helper'
7 require 'rspec/rails'
8
9 require 'capybara/rspec'
10 require 'capybara/rails'
11
12 Capybara.javascript_driver = :webkit
13 Category.delete_all; Category.create
14 Shoulda::Matchers.configure do |config|
15   config.integrate do |integrate|
16     with.test_framework :rspec
17     with.library :rails
18   end
19 end
20
21 # Add additional requires below this line. Be sure to
22 # require supporting ruby files with appropriate
23 # spec/support/ and its subdirectories. These files
24 # run as spec files by default. This means you can
25 # in _spec.rb will both be required and run
26 # run twice. It is recommended that you
27 # end with _spec.rb. You can configure the
28 # option on the command line via --require
29
30 No results found for 'mongoid'
```

The HIPAA Security Rule requires all security incidents to be reported to the HIPAA Compliance Officer immediately.

This can assist in determining if and when a data breach occurred.

This is also helpful for a starting point in case something is determined "later".



What is a security incident?

A security incident under 45 CFR § 164.304 is defined as the **attempted** or **successful** unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

Additionally, 45 CFR § 164.308(a)(6)(ii) requires business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes; and must report security incidents to its covered entity.

Documenting security incidents

Security Incident Report	
---------------------------------	--

Name of Facility: _____ Date of Incident: _____

Name of person reporting the incident: _____

Security Incidents can lead to a Breach of Protected Health Information. Types of Security Incidents could be something as simple as an unusual pop-up, a computer screen that freezes, your password no longer works, or it could be much more, like a lost or stolen laptop, flash drive, desktop, or server. Each incident must be reported to the Security Officer immediately.

Type of Security Incident:

Paper chart	
Workstation	
Laptop	
Tablet/Smart phone	
Other:	

Explain:

What type of Protected Health Information was involved?

Paper	
Electronic	
Sensitive PHI	
None	

If the answer above is anything but NONE, please complete the rest of the report.

- This incident involves less than 500 patient records
 This incident involves more than 500 patient records

Some data breaches are a result of lost or stolen devices; law enforcement may be asking if the device was used in a healthcare setting.

If yes, the next question will be, was it encrypted?

If the answer is yes, nothing further is needed.

If the answer is no, more than likely the OCR will be contacted, and an investigation will be opened.

RISK ASSESSMENT

1. Was the PHI viewed, accessed, or acquired?

Explain:

2. Who was the unauthorized person or entity that accessed the PHI?



Avoiding security incidents

- Let IT install updates. Do not click on a pop-up, because one click can infect your system with malware or a virus.
- Do not click on any links in an email, open your web browser and go to the website directly.
- Do not plug in any USB drive without knowing where it came from.
- If an email or a phone call asks you to do something immediately, DON'T. Verify what they are asking for.
- Phone calls warning you of a new virus and offering a “free” scan - NEVER allow anyone access that is not authorized to do so.



Facility controls

HIPAA also addresses the needs of physical security.



Using security systems that can track access through logs or security cameras can demonstrate best practices and could help to avoid a class action lawsuit should a theft occur.





Reporting data breaches

Once it has been determined that a security incident is a data breach, it must be reported to the Office for Civil Rights. Depending on the number of patient records that are affected will determine the timing of the reporting.

For example, under 500 patient records, you must report the breach within 60 days after the last day of the year that the breach occurred. You may also file the report during the same year.

For data breaches over 500 patient records, this must be reported within 60 days of the breach, unless state law has a lesser time frame. The only exception is if the data was encrypted, or it can be confirmed the data was not accessed or viewed. If reporting impedes a police investigation, the time may be extended.

Check your state laws, since you may be required to report this to the State Attorney General as well.

What is Phishing?



Enter your login information:

User name:

Password:

OK

Cancel

There are two main types of phishing, regular phishing and spear phishing.

Regular phishing is when an employee received an email, text, or phone call asking for information immediately.

Spear phishing is when they target C level or management.

The goal is always to gain valuable information!

9:52



10:01



10:01



safetytransactionswellsfarg087935... >

Text Message
Yesterday 7:37 PM

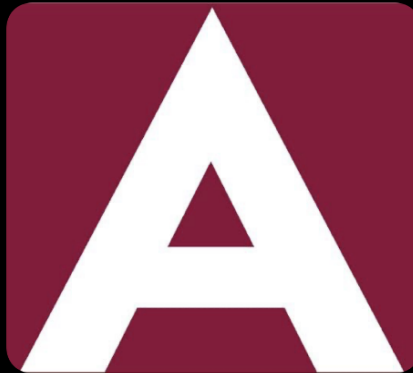
(Get in touch: [8669661263](tel:8669661263))
#Vvfx-9712 Your CARD is temporarily unavailable for usage. 7:36:08 PM

The sender is not in your contact list.
[Report Junk](#)



+1 (727) 310-7408 >

Text Message
Fri, Aug 25 at 6:53 PM



{ACHIEVA CU} There is a new request to initiate transfer of \$507 if not recognize review <https://achfclu.online> now

The sender is not in your contact list.
[Report Junk](#)



+1 (313) 980-3515 >

Text Message
Mon, Aug 28 at 1:15 PM



•{ACHIEVA CU} ~A New transaction was added to your Bill pay; if this was done in an error, Visit Here <https://disputeachievaclu.online/> to Cancel

The sender is not in your contact list.
[Report Junk](#)

Text Message

Text Message

Text Message

Do not CALL or CLICK on any of these!



Email phishing example

TRUIST 

An update on your Truist account

This is an automated message. Please do not reply directly to this email.

UPDATE INFORMATION NOTICE

DEAR VALUED CUSTOMER,

We see you still have some tasks left on your "To-Do List." We need you to complete these items so we can finish the final review of your account.

This should take you just a few minutes. Simply sign into your account and complete the outstanding <https://trulioa.com/app/new-recently>

completed all your tasks. [Click to follow link](#) promptly!

[Finish To-Do List](#)

Once the final review is complete and investors have backed your loan you'll be ready to go.


Truist Alerts

Need additional assistance? Visit [help](#) &

Always hover over the "From" email and make sure it is actually from the person or company you are familiar with. The difference could be a simple "." in the URL address.

"We noticed you have some tasks left on your "To-Do-List" If you hover over the "Finish to-do List" you will see it takes you to a different website.

The goal is to get you to click on the link.



What to do next

If someone has clicked a link or opened an attachment that downloaded harmful software:

- Contact your IT department to update your computer's security software.
- They will run a scan and delete anything it identifies as a problem.

If you think a scammer has your information, like your Social Security, credit card, or bank account number:

- Go to [identitytheft.gov](https://www.identitytheft.gov) for steps you can take based on what kind of information was lost or exposed.

If you gave your username and password to a scammer:

- Change your password right away. If you use the same password for other accounts or sites, change it there, too.

If someone calls and offers to "help" you recover money you have already lost:

- Don't give them money or personal information. You are probably dealing with a fake refund scam.

Who to contact?

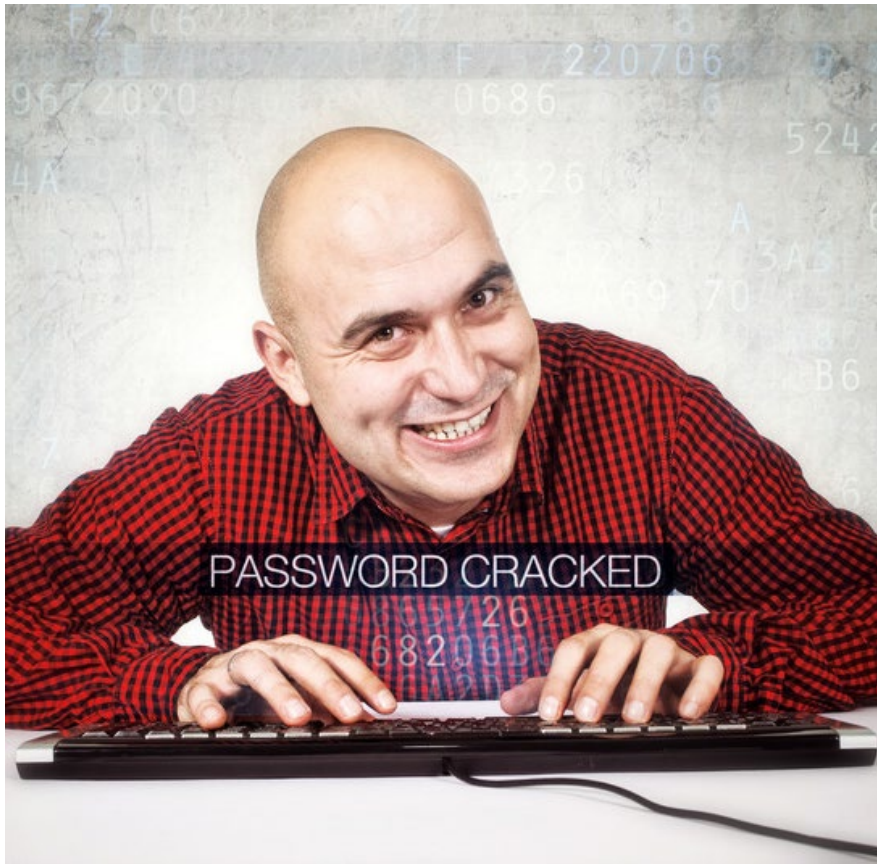


FEDERAL TRADE COMMISSION
[ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)

When you receive an email, text, or phone call, you should call your bank or the company to advise them of what happened. If they are doing this to you, they are doing this to **MANY** others. Also, you can report this to the Federal Trade Commission (FTC).

NOTE: The FTC does not resolve individual reports, but your report will be entered in the FTC's Consumer Sentinel database and will be available to federal, state, and local law enforcement across the country.

Password management



Strong passwords or phrases must be utilized, minimum of 8 characters, upper and lower case, and at least one number and one special character.

For example:

Wh3r3areMYk3ys!

!l0stMyP@\$w0rd#

Best practice is to change every 90 days or add a multi-factor process!



Workstation use

Remind your staff that workstations are to be used for the sole purpose of performing their job function. This is critical because by visiting certain websites such as a recipe site, clicking on links in emails and Facebook can infect your network.

Cell phones can cause distractions and HIPAA violations when used improperly. It also causes patients to be untrusting and may lead to a patient complaint. Best practices are for the staff to give out your office number. Many practices now offer cell phone lockers.

Personal devices should use a guest network that is outside of where ePHI is located or accessed.

Workstation security



USB ports pose an opportunity for patient data to be downloaded or to infect the network. Therefore, should be disabled or locked if they are not used. Alternatively, you could routinely check for unauthorized devices.

Portable devices should be secured if left unattended.

Privacy screens should be used on all workstations that are located where it can be viewed by unauthorized persons. Even if it across the room!



Mobile device management

The HIPAA Security rule requires that all devices that contain or access ePHI be secured.

It is recommended that all devices that contain or access ePHI should have remote wipe or auto wipe capabilities, unless it is encrypted.

All devices should be maintained by an IT professional to ensure that all security updates are current and virus free.

If a device is lost or stolen it must be reported to the HIPAA Compliance Officer IMMEDIATELY!

Remote users



NEVER use a Public Wi-Fi, criminals can spoof legitimate networks to steal information.

It is best to use a VPN (Virtual Private Network) that has been set up by your IT professional.

When using Wi-Fi be sure to use the latest encryption and a separate Wi-Fi connection from the rest of the family.

Never leave a laptop or portable device in a car or unattended.

Device & media controls



The Compliance Officer is responsible for the documentation of all equipment that accesses or stores PHI.

This is known as an inventory list and should be updated regularly.

Equipment that accesses or has stored ePHI must be handled properly BEFORE re-using, donating, or destroying the device.



Access controls



Users should log off their workstations when they walk away. (Ctrl, Alt, & Delete, then choose Sign out).

Also, the Auto-Log off feature in the EHR system or operating system should be engaged. This is helpful in the event the user forgets to log off. Time limit could be 10 minutes in controlled areas, and 3 minutes in uncontrolled areas.

(This includes remote users)

If this hampers the workflow, an RFID card or bio-metric reader may be utilized.



User authentications



Two factor authentication is required under HIPAA. This means entering a username and password. Passwords are to be secured and never shared.

A second authentication process should be implemented when possible and on portable devices as well as for remote users. This could be the use of a code authenticator, the answer to a question, or a code sent to a mobile device or email.

If a mobile device or email is utilized, it is critical to ensure a second authentication method is used on the device or account as well.



Transmission security



HIPAA permits the use of email provided it is encrypted. If encryption is not available, and the patient has been advised that this method is not secure, you are permitted to send PHI unencrypted if the patient agrees to it. Be sure to retain their authorization or email.

When communication via text and PHI is involved, this method should be encrypted as well.



Who must not work in Healthcare?

The Office of the Inspector General (OIG) investigates fraud, waste, abuse, and mismanagement in the U.S. Department of Health and Human Services' programs. Anyone that has participated in these activities is forbidden to work in healthcare and may face jail time and be forced to pay restitution.

The OIG maintains a list of all currently excluded individuals and entities. It is required to check this list before a person/company is hired and the list must be checked on a regular basis.

This is called the List of Excluded Individuals/Entities (LEIE).

Those that are excluded cannot receive payments from Federal health care programs for any items or services they furnish, order, or prescribe.

Who enforces HIPAA?



The Office for Civil Rights (OCR), a division of The Department of Health and Human Services is the agency that investigates and enforces HIPAA violations since privacy is a Civil Right.

Non-compliance is a civil offense that carries penalties ranging from \$137* to \$68,928* per violation. There are caps on identical violations ranging from \$34,464* to \$2,067,813*.

* Depending on the type of violation and subject to increases



HIPAA Violations in the News:

Covered Entities:

- Lost unencrypted laptop. \$3M
- Hacking incident \$1.5M
- Sharing PHI without BAA \$500K
- Improper disposal of PHI. \$300K
- Negative response to online review. \$30K
- Patient Right of Access violations from \$5K-\$200K

Business Associates:

- Misconfigured network \$3M
- Compromised credentials \$2.3M
- Lost mobile device \$650K
- Unsecured network \$350K
- Network ransomware. \$100K
- Cyber-attack \$100K
- Unsecured network exposing only 267 records. \$75K

Read about resolution agreements:

<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>



Recognized Security Practices

These RSPs are recommended in NIST and the Security Rule. This can be defined as reasonable and appropriate security measures based on the size of your organization.

Each organization must assess their environment and adapt “best practices”. Compliance Officers should review the OCR Recognized Security Practices Video Presentation:

<https://www.youtube.com/watch?v=e2wG7jUiRjE&t=955s>

The OCR may conduct a minimum of a one year look back on your documented compliance efforts.

Documentation is the key!

Reasonable and Appropriate



- Cost is a factor
- Size doesn't matter
- How you store your data
- Policies and Procedures
- Documentation is everything!

What is Information Blocking



Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception.

The "actors" definition under the Cures Act applies to healthcare providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs).



When does the Law Apply?

The law applies whether the actors know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI.

For healthcare providers, the law applies whether they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.





Patient Requests



PATIENT'S BILL of RIGHTS

Patients may request their information in the format of their choice and to be sent to whoever they authorize.

This includes third party electronic vendors and even mobile apps.



Check the availability

When a patient requests access or to share their information, if the staff member is unsure about the request, they should advise the patient they will check the availability of their request with their compliance officer.

Depending on the method of access or transfer, it may or may not be feasible at that time.

**Remember,
NEVER just say NO!**

This could be considered information blocking!





Information Blocking exceptions

Exceptions are divided into Two Categories

Exceptions that involve not fulfilling a patient's request to access, exchange, or use EHI.

- Preventing harm
- Privacy
- Security
- Infeasibility
- Health IT Performance


Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

- Licensing
- Fees
- Content and manner

When these practices meet the conditions of one or more exceptions, this would not be considered information blocking.



Online Tracking Technology



The Office for Civil Rights (OCR) has teamed up with the Federal Trade Commission (FTC) to investigate healthcare websites for the use of Online Tracking Technology.

Some medical marketing and website designers are not up to date with the HIPAA requirements.



Human Trafficking

The U.S. Department of State defines human trafficking as an activity in which someone obtains or holds a person in compelled service. The term covers forced labor and forced child labor, sex trafficking, including child sex trafficking, debt bondage, and child soldiers, among other forms of enslavement.

It is estimated that 27.6 million victims trafficked every year worldwide. The majority of whom are women and children.

Some states require annual human trafficking training. Check your state laws.

Here are some resources:

<https://www.aha.org/system/files/media/file/2021/01/Introduction-to-Human-Trafficking-and-Health-Care-Providers-Legal-Requirements-for-Reporting-and-Education.pdf>



HELP!



Have you conducted a system wide Risk Analysis that includes Administrative, Physical and Technical safeguards?

Have you created a Risk Management Plan from your Risk Analysis?

Do you have written Policies & Procedures that cover all the HIPAA Rules?

Do you understand network security?

Do you need some help?



Q & A



Aris Medical Solutions developed an online HIPAA compliance management system called the *HIPAA Keeper™*.

Aris has changed the way medical professionals handle their regulatory requirements by keeping HIPAA documentation in an organized system to save time and money.

To learn more or schedule a demo:
Suze Shaffer, CHSP
HIPAA Security Analyst
info@arismedicalsolutions.com
877.659.2467