

HIPAA Compliance Officer Training

By HITECH Compliance Associates



Building a “Culture of Compliance”



Your Instructor Is Michael McCoy
Nationally Recognized HIPAA Expert

SUBJECTS COVERED

1. OCR Access Guidance
2. Business Associates
3. Importance of Cybersecurity Training
4. Reasonable & Appropriate Security
5. Breach Notification Rule
6. Enforcement Rule
7. Information Blocking



DHHS – Department of Health & Human Services
CMS – Centers for Medicare and Medicaid Services
OCR- Office for Civil Rights
ONC – Office of the National Coordinator
OIG – Enforces Information Blocking
TPO – Treatment, Payment, and Health Care Operations
PHI – Protected Health Information
ePHI – Electronic Protected Health Information
Sensitive PHI (sPHI) – Special Class of PHI
Malware – All Classes of Malicious Software
MIPS – EHR Requirements for Stimulus Funds
Willful Neglect - Conscious, Intentional Failure or Reckless
Indifference to the Obligation to Comply with HIPAA



Information Blocking

21st Century Cures Act

Section 4004

Tidal Wave of Change

This webinar is not intended to be legal advice. We are not attorneys.

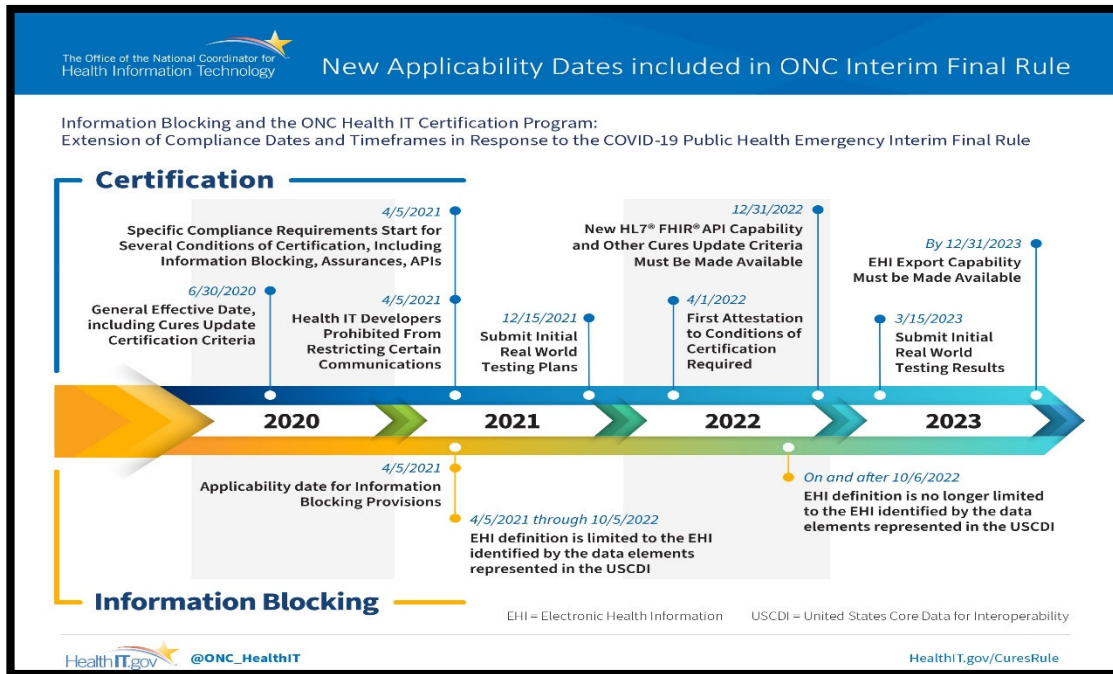
The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state and local laws may also apply.

We will learn more as the 320-page Rule is implemented. There is limited information on the aggressiveness of enforcement.



Legislative History

Report to Congress in 2015 by Office National Coordinator (ONC) on the state of health IT.
 21st Century Cures Act passed in 2016



Bipartisan Bill

Access and Control By Patients



Enforcement

In the context of information blocking, the Cures Act authorizes CMPs for:

Any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information if this practice is conducted by a developer of certified health information technology (health IT), an entity offering certified health IT, a health information exchange, or a health information network, and the developer of certified health IT, entity offering certified health IT, health information exchange, or health information network knows or should know that this **practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information.**

**Appropriate Disincentives – Health Care Providers
(ONC has not published actual disincentives to be applied)**

Civil Monetary Penalties – Up to \$1,000,000 per violation



Harm / Damages are not a requirement for you to be an information blocker and fined with appropriate disincentives.

It is Information Blocking to prevent or discourage patient access.

OCR Settles Seventeenth Investigation in HIPAA Right of Access Initiative



OCR HIPAA Privacy Rule information distribution <OCR-PRIVACY-LIST@LIST.NIH.GOV> on behalf of OS OCR PrivacyList, OCR (HHS/OS) <OCRPR To: OCR-PRIVACY-LIST@LIST.NIH.GOV

Reply Reply All Forward ...

Wed 3/24/2021 1:48 PM

HHS Office for Civil Rights in Action



March 24, 2021

OCR Settles Seventeenth Investigation in HIPAA Right of Access Initiative

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services announces its seventeenth settlement of an enforcement action in its HIPAA Right of Access Initiative. OCR announced this initiative to support individuals' right to timely access to their health records at a reasonable cost under the HIPAA Privacy Rule.

The Arbour, Inc., doing business as Arbour Hospital ("Arbour"), has agreed to take corrective actions and pay \$65,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Arbour is located in Massachusetts and provides behavioral health services.

In July 2019, a complaint was filed with OCR alleging that Arbour failed to take timely action in response to a patient's records access request made in May 2019. OCR provided Arbour with technical assistance on the HIPAA Right of Access requirements. Later, in July 2019, OCR received a second complaint alleging that Arbour still had not responded to the same patient's records access request. OCR initiated an investigation and determined that Arbour's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard, which requires a covered entity to take action on an access request within 30 days of receipt (or within 60 days if an extension is applicable). As a result of OCR's investigation, Arbour provided the patient with a copy of their requested records in November 2019, more than 5 months after the patient's request.

"Health care providers have a duty to provide their patients with timely access to their own health records, and OCR will hold providers accountable to this obligation so that patients can exercise their rights and get needed health information to be active participants in their health care," said Acting OCR Director Robinsue Frohboese.

In addition to the monetary settlement, Arbour will undertake a corrective action plan that includes one year of monitoring. A copy of the resolution agreement and corrective action plan may be found at <https://www.hhs.gov/sites/default/files/arbour-racap.pdf>.*

*People using assistive technology may not be able to fully access information in this file. For assistance, contact OCR at (800) 368-1019, TDD toll-free: (800) 537-7697, or by emailing OCRMail@hhs.gov.



**“Power to the Patient.
Our Records.
Our Right.
Our Choice.”**

Deputy National Coordinator for Health Information Technology,
Steve Posnack stated the impact of the Cure’s Act this way.

**Cultural Change for
Actors.**

ONC goal to put
patients in control.

Based on request of
the patient. What
constitutes a
Request? How long is
the request good for?

Regulations go from can
share to must share.

Focus Of This Webinar is Health Care Providers

Actors – Health Care Providers: Same meaning as “health care provider” at 42 U.S.C. 300jj



Health Care Providers

Who are they?

- a hospital
- skilled nursing facility
- nursing facility
- home health entity or other long term care facility
- health care clinic
- community mental health center
- renal dialysis facility
- blood center
- ambulatory surgical
- emergency medical services provider
- federally qualified health center
- group practice
- a pharmacist
- a pharmacy
- a laboratory
- a physician
- a practitioner
- a rural health clinic
- an ambulatory surgical center
- a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization
- a “covered entity” under certain statutory provisions
- a therapist
- any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary

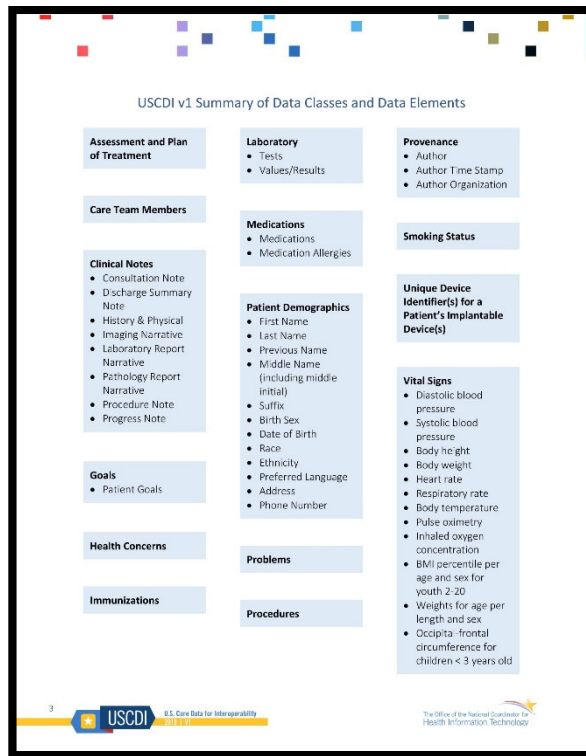
Other Actors Include:

Health IT developers of certified health IT; and
Health Information Networks (HINs) or HIEs (HIN and HIE are combined into one defined type in the Final Rule).

Even if you are not a HIPAA Covered Entity, you are still covered by Section 4004, Information Blocking.

Definition of EHI for 1st Two Years

The USCDI v1 is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.



U.S. Core Data for Interoperability- USCDI – only EHI that is subject to Information Blocking until May 2, 2022

Patient’s can still order full medical record under HIPAA statutes that must be fulfilled within 30 days. (Proposed Rule in progress limits to 15 days.)

USCDI does not contain billing/payment information.

Assessment and Plan of Treatment

Care Team Members

Clinical Notes

Goals

Health Concerns

Immunization

Laboratory

Medications

Patient Demographics

Problems

Procedures

Provenance

Smoking Status

Unique Device Identifiers for Implantable Devices

Vital Signs

Information Blocking

INTERFERE

Except as required by law or covered by an exception, is **likely** to **interfere** with access, exchange, or use of electronic health information (EHI).

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule | Information Blocking

The Office of the National Coordinator for Health Information Technology

Interfere with Access, Exchange, or Use

“Interfere with, prevent, or materially discourage”

- The terms “interfere with” and “interference” are used inclusive of prevention, material discouragement, and other forms of interference that implicate the information blocking provision.
- We interpret “interference” broadly and to take many forms.

Delays -An actor’s practice of slowing or delaying access, exchange, or use of EHI could constitute an interference and implicate the information blocking provision.

Costs for Electronic Access by

Patients/Individuals-An actor’s practice of charging an individual, their personal representative, or another person or entity designated by the individual for electronic access to the individual’s EHI would be **inherently suspect** under an information blocking review.

Correspondence

Must send letter to patient within 10 if apply law or exemption to deny access.

Information Blocking

1. **Practices** that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law;
2. **Implementing health IT in nonstandard ways** that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI;
3. **Limiting or restricting the interoperability of health IT, such as disabling or restricting the use of a capability that enables sharing EHI with users of other systems or restricting access to EHI by certain types of persons or purposes that are legally permissible, or refusing to register a software application that enables patient access to their EHI** (assuming there is not a legitimate security reason that meets the conditions of the Security Exception, discussed further below);



API
Application
Programming
Interface

Information Blocking

4. *Implementing health IT in ways that are likely to restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems. This would include acts that make transitions between certified health information technologies more challenging (e.g., an EHR vendor charging excessive fees or using tactics to delay a practice's switch from their EHR to another vendor's EHR);*

5. **Acts that lead to fraud, waste, or abuse, or impede innovations and advancements** in health information access, exchange, and use, including care delivery enabled by health IT;

6. **Restrictions on access, exchange, and use, such as may be expressed in contracts,** license terms, EHI sharing policies, organizational policies or procedures or other instruments or documents that set forth requirements related to EHI or health IT, such as Business Associate Agreements (BAAs); and

7. *Rent-seeking (e.g., gaining larger profits by manipulating economic conditions) or other opportunistic pricing practices.*

Information Blocking

Formal restrictions: **Policies Restricting:** *Provider or office policy requires staff to obtain a patient's written consent before sharing any EHI with unaffiliated providers for treatment purposes.*

Informal: Providing Information in Unusable Format

Disabling Interoperability – Making it generally difficult to access and share.

Technical limitations: A physician disables the use of an EHR capability that would enable staff to share EHI with users at other systems.

Isolated interferences: **A physician has the capability to provide same-day EHI access in a format requested by an unaffiliated provider—or by their patient—but takes several days to respond.**



Physicians are required to follow state or federal laws applicable to the release of medical records.

High Risk Information Blocking Activities

Inherently Suspect Activities

Interference with:

Patients seeking to access their own EHI;

Providers requesting medical records for treatment or health care operations;

Payers who seek EHI to confirm a clinical value;

Patient safety and public health.



Examples of Information Blocking

Office Policies that are More Restrictive than HIPAA

Requiring a signed Authorization to share records for Continuity of Care
Exception: Security?

Creating Hurdles to Access or Exchange EHI

Misunderstanding the Law

Applying (claiming) HIPAA restricts when no legal claim exists.

Slowing or Delaying

Taking more than a day or not having records immediately that had been “requested”.

Not Entering Data into EHR when HIPAA Allows

Make sure data is entered timely.

Slowing or delaying could be Information Blocking.

Request Made: As soon as is available.

No Indication as to what a “delay” time frame would be.

Immediate is the expectation.

ONC will not tell you in advance if you are information blocking.

Examples of Information Blocking

Time Frames Provided by Other Laws

Under Information Blocking you do not have the 30 days allowed by HIPAA.

Provider to Provider Request for Records

Unlike HIPAA where regulation outlines when information is **permitted** to be exchanged, info blocking regulations **are directive and require** Actors to provide access, exchange, and use of EHI for nearly all requests.

Physician wants to Review Before Releasing Records

This could be considered an unreasonable delay.

Test Results

If **requested**, results need to be available as soon as you receive them.

Available Upon Request

Do you have the technology to complete immediately?

Patient Is In Control

Patient Should
Receive Information
at the Same Time

An Act or Omission
Could Be
Information Blocking

Examples of Information Blocking

If You Have the Capability You Would Need to Explain Why Not Available.

Why are you not pushing records to your portal.

Not Interfacing with Certified APIs and TEFCA Networks.

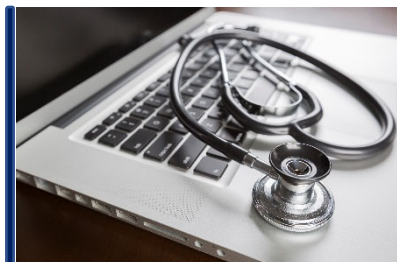
Application Program Interface for patient access via an app.

Contractual Restrictions Can Constitute Information Blocking.

Share the Information Unless You Have a “Good” Reason Not to Share the Data.

Document.

Use of any Exemptions, laws or other reason not to disclose.



FAQ

Interference

Q: Do the information blocking regulations (45 CFR Part 171) require actors to proactively make electronic health information (EHI) available through “patient portals,” application programming interfaces (API), or other health information technology? *1/15/2021*

No. There is no requirement under the information blocking regulations to proactively make available any EHI to patients or others who have **not** requested the EHI. We note, however, that a delay in the release or availability of EHI in response to a request for legally permissible access, exchange, or use of EHI may be an interference under the information blocking regulations ([85 FR 25813](#), [25878](#)). If the delay were to constitute an interference under the information blocking regulations, an actor’s practice or actions **may** still satisfy the conditions of an exception under the information blocking regulations ([45 CFR 171.200-303](#)).



REQUEST

ONC FAQ - Example

It would likely be considered an interference for purposes of information blocking if a health care provider established an organizational policy that, for example, imposed delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results (see also 85 FR 25842 specifying that such a practice does not qualify for the “Preventing Harm” Exception).

To further illustrate, it also would likely be considered an interference:

where a delay in providing access, exchange, or use occurs after a patient logs in to a patient portal to access EHI that a health care provider has (including, for example, lab results) and such EHI is not available—for any period of time—through the portal.

where a delay occurs in providing a patient’s EHI via an API to an app that the patient has authorized to receive their EHI.



Exemptions to the Definition of Information Blocking

Preventing Harm Exception

It will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.

Privacy Exception

It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.

Security Exception

It will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.

Content and Manner Exception

It will not be information blocking for an actor to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met.

Very Limited.

Follow HIPAA Exemptions

Case by Case

Determination with Appropriate Documentation

High Bar is set for any Exemption to be applied.

Exemptions to the Definition of Information Blocking

Health IT Performance Exception

It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

Infeasibility Exception

It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.

Fees Exception

It will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.

Licensing Exception

It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.

Very Limited.

Follow HIPAA Exemptions

Case by Case Determination with Appropriate Documentation

You are Expected to be Able to Reach Reasonable Terms for Manner Requested.



Report information blocking



Report Information Blocking

In your submission, please consider including information that will help us understand the concern(s) you are reporting. Examples of information that would be particularly helpful would include, but not be limited to:

- Person or entity that requested access, exchange, or use of electronic health information (EHI)
 - Role of person/entity (e.g., patient, health care provider, health information network/exchange (HIN/HIE), health IT developer of certified health IT)
 - Date and time of request
 - Location of requestor (city, state)
- Type of EHI requested (e.g., lab result, medical history, diagnostic images)

Formatting Help

Create

Cancel

Information Blocking Compliance Kit

Documentation is key to compliance.

Action Plan for Compliance – Information Blocking Framework

Policies and Procedures need to be developed for consistent application of the rules.

Exemptions Forms – If an exemption is taken, it must be documented to the standards for the specific exemption.

Response Letters – Required within 10 days of “request”.

Training/Education – Management must know and understand what the government feels are practices that would lead to a claim of information blocking.

Support – We are at the beginning of major and sweeping regulations. Questions will arise as this legislation and implementation proceed.

Updates: Actual enforcement actions and additional guidance will help us keep your office updated.

Get order
information on our
web site
[www.
HIPAAComplianceKit
.com](http://www.HIPAAComplianceKit.com)

Or Call:
813-892-4411

Willful Neglect



Minimum Mandatory Fines. \$25,000 to \$16,000,000.

1. Not Performing **Risk Assessments** on a Regular Basis
2. Not Having a Complete Set of **Policies and Procedures**
 - a. Privacy Rule
 - b. Security Rule
3. Not **Training** Your Staff on Your Policies and Procedures

Small Practice can expect \$100,000 fine if caught without Security Risk Analysis





Permitted Disclosures

HIPAA provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities without first obtaining an individual's authorization: including for treatment, payment and for health care operations.

STEP 7 – Documentation

Required Postings

Last Year's Audits Showed Up to 94% Failure to Comply

Lobby

Post Notice of Privacy Practices

Non-Discrimination Notice (Section 1557)

Pricing for Medical Records (if not posted on web site)

Web Site – Must be Prominent

and Downloadable

Privacy Policy of Web Site

Notice of Privacy Practices

Pricing for Medical Records

Non-Discrimination



Notice of Privacy Practices

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

<p>Your Rights You have the right to:</p> <ul style="list-style-type: none"> • Get a copy of your paper or electronic medical record • Correct your paper or electronic medical record • Request confidential communication • Ask us to limit the information we share • Get a list of those with whom we've shared your information • Get a copy of this privacy notice • Choose someone to act for you • File a complaint if you believe your privacy rights have been violated 	<p>Your Choices You have some choices in the way that we use and share information as we:</p> <ul style="list-style-type: none"> • Tell family and friends about your condition • Provide disaster relief • Include you in a hospital directory • Provide mental health care • Market our services and sell your information • Raise funds
<p>Our Uses and Disclosures We may use and share your information as we:</p> <ul style="list-style-type: none"> • Treat you • Run our organization • Bill for your services 	<ul style="list-style-type: none"> • Help with public health and safety issues • Do research • Comply with the law • Respond to organ and tissue donation requests • Work with a medical examiner or funeral director

When it comes to your health information, you have certain rights. This notice explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask us for an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy of a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to amend your medical record

- You can ask us to amend health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may not "amend" your request, but we'll tell you why by writing within 60 days.

Request confidential communication

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will not "opt" or "unsubscribe" requests.

Ask us to limit what we share

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may not "opt" if it would affect your care.
- If you pay for a service or health care item out of pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will not "opt" unless a law requires us to share that information.

Get a list of those with whom we've shared information

- You can ask us for a list of the names of the ones we've shared your health information for no more than 60 days after the date you ask us how to do this, and why.
- We will include all the third parties except for those other treatment, payment, and health care operations, and certain other disclosures (such as any we asked to make). We'll provide one summary page for each third party, if possible, and those for whom we don't have that information.

Get a copy of this privacy notice

- You can ask for a paper copy of this notice at any time.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. We will assume the person has this authority unless you take any action.

Your Choices

In certain health information, you can tell us your choices about what we share. If you have a choice, we will let you know about your choices and how to make them. Tell us how to do this, and we will follow your instructions. In these cases, you have both the right and choice to tell us:

- Share information with your family, close friends, or others involved in your care.
- Share information to disaster relief efforts.

If you are not able to tell us your preferences we may go ahead and share your information if we believe it is your best interest. We may also share your information when needed to ensure a serious and imminent threat to health or safety.

Your Health & Right to File a Complaint if You Don't Have Privacy Has Been Violated

- If you feel your Privacy Rights have been violated, please call our toll-free Privacy Complaint Line. Our Privacy Office will review your concern and promptly notify you of the actions our office will take.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-684-6772, or visiting www.hhs.gov/officeforprivacy.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We will notify you if we learn of a breach that may have affected your information.
- We will not use or share your information other than as described here unless you tell us or we can no longer find you to do so.
- We may change this notice from time to time. Let us know in writing if you change your email.
- For more information on our health privacy practices, please contact our privacy officer.

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. We will notify you in writing if we make any changes to this notice, and we will post the updated notice on our website.

Your Medical Practice
HIPAA Compliance Officer: Gina Ireland
Phone: 613-222-4444
This Notice of Privacy Practices is effective January 1, 2016.





Every Covered Entity Must Have A Responsible Person

HIPAA Privacy Officer

HIPAA Security Officer

Commonly known as the

HIPAA Compliance Officer

These are not just job titles, the position has responsibilities under federal law.



COMPLIANCE
REGULATIONS
GUIDELINES

“Everything, pretty much, must be in writing.”



OCR Guidance Enacted In 2017



A Patient's Right to Access

Major Provisions

1. Designated Record Set
2. Fees
3. Timeliness
4. Format
5. Email
6. **Access** Directly



Cannot Create A Burden or Delay

A covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require an individual:

- 1) Who wants a copy of her medical record mailed to her home address to physically come to the doctor's office to request access and provide proof of identity in person.
- 2) To use a web portal for requesting access, as not all individuals will have ready access to the portal.
- 3) To mail an access request, as this would unreasonably delay the covered entity's receipt of the request and thus, the individual's access.

OCR Guidance from 2017

Fees:

- 1) \$6.50 Flat Fee
- 2) Actual Costs
- 3) Average Costs

*OCR says have your cost documentation.
You must provide upon request.*



Patient Copying Charge Notification Sheet

Average Cost Method

PRICING FOR PATIENTS ONLY, NOT REQUIRED FOR 3RD PARTY REQUESTS INCLUDING ATTORNEY REQUESTS FOR RECORDS

Paper Copies of Medical Records

(Fees for Quality Assurance, Fulfillment and Billing & Scanning)
Request, Intake, Verification, Compilation and Determination – No Charge Per the HIPAA Regulations

1 Staff Time Charges to Complete Request							
		Average Time	Time Charge	Fee no scanning	Scan Time	Fee w/ Scanning	
Pages	1 - 25	20	.37 min	\$7.40	4 min	8.88	
	26 - 50	26	.37 min	\$9.62	7 min	12.21	
	51 - 75	32	.37 min	\$11.84	10 min	15.54	
	76 - 100	38	.37 min	\$14.06	13 min	18.87	
	100+	50	.37 min	\$18.50	16 min	24.42	
Select Fee From Above						Time Fees	

2 Costs for Supplies – Paper and Toner			
Number of Sheets of Paper		x .10/page	= Total Supplies \$

3 Postage (if Applicable)			
Actual Cost of Postage and Mailing Supplies		Total Postage	\$

Calculation of Total Fees for Medical Records Request (per HIPAA Guidelines)

1	Time Fee	
2	Supplies Fee	
3	Postage	
4	Other Costs for This Request	
Total Charges		\$

Digital Copies of Medical Records

Email	Patient Warned of Risks	Flat Fee	\$6.50
CD	Sent Media Mail	Flat Fee	\$6.50
Thumb Drive	Sent Media Mail	Average Cost	\$25
Patient Portal			No Charge
Transfer of Records For Continuity of Care			No Charge
Total Charge			\$

Practice		
Records Request for:		Z# Identifier

HIPAA Compliance Kit Form – Step 7: Documentation: HCO Forms: Patient Copying Charge Notification Sheet

Fees:

The fee **may not include** costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above ***even if*** such costs are authorized by State law.

OCR Guidance from 2017



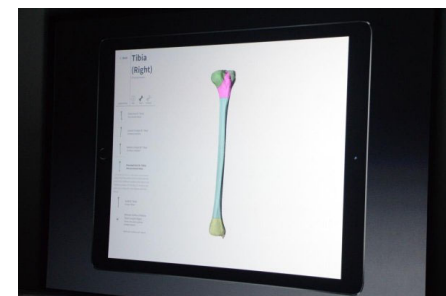
Timeliness

In EHR – Immediately?

Make sure you are complying with “MIPS”.

Current Rules

30 days plus 30 if off-site.



OCR Guidance from 2017



Format

You Are Required to Provide All Formats That You Can Readily Produce.

Thumb Drive, CD, Email



OCR Guidance from 2017



Emailing of PHI

You Must Email Records Upon Request

Protections must be in place and documented.

Using secure email to patients will cost you time.



OCR Guidance from 2017



Patient Can Direct to Any 3rd Party

Dxwkrul}dwlrq#rup #Jhtxluhg#ru#Dq|#
Glvforvxuhv#R xwlg#h#i#F rqlwxlw|#r i#F duh|1

OCR Guidance from 2017



Patient Can Direct to An App

You Must Send to 3rd Party Apps
If You Have the Capability.

Use Authorization Form.



OCR Guidance from 2017

Access Directly

Patients Have a HIPAA Right to Access their PHI As It Is Maintained in Your Electronic Medical Records and Practice Management System.

Set Up A Station For Viewing Medical Records.

Patient Is Allowed To Take Photos of Screens

No Fees or Charges Allowed.

May Be Allowed to Access Business Associate Computers.



OCR Guidance from 2017











Cannot Require Patient To Use Portal

That Could Create A Burden.

HIPAA Compliance Kit
HIPAA.Omnibus Compliance System

COMPLIANCE
REGULATIONS
GUIDELINES

 STEP 1	Risk Assessment
 STEP 2	Business Associates
 STEP 3	Policies & Procedures
 STEP 4	HIPAA Training
 STEP 5	Breach Plan
 STEP 6	Contingency Plan
 STEP 7	Documentation
 STEP 8	System Activity Review

STEP 1 – Risk Management

Risk Management

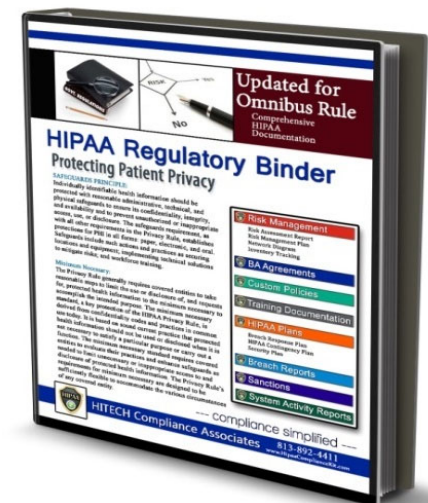
Risk Assessment

Required Yearly – Document known vulnerabilities

Risk Management Report

Required Yearly – Manage known vulnerabilities

2019 – SRA Required Before You Can Meet Requirements for Promoting Interoperability. 7%+ Reduction in Medicare/Medicaid.



STEP 1 – Risk Management

Risk Management

\$5,550,000 Fine

“Two major cornerstones of the HIPAA Rules were overlooked by this entity. Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure.”

Jocelyn Samuels,
Former Director of the U.S. Department of Health and Human Services (HHS)
Office for Civil Rights (OCR)



STEP 1 – Risk Management

Risk Assessment Risk Management Report

The **HITECH Security Framework Risk Assessment** is the most comprehensive risk assessment for HIPAA compliance available. It is built from the following sources: the NIST Cybersecurity Framework, NIST Guide for Conducting Risk Assessments, GAO Information Security Risk Assessment – Practice of Leading Organizations, CMS Information Security Series, CMS Information Security ARS, Baldrige Excellence Framework, CIS Security Controls and Guidance from the OCR on performing risk assessments. These resources make the HITECH Security Framework Risk Assessment the established standard in the development of your personalized Risk Management Plan.



STEP 1 – Security Risk Assessment

MIPS-eligible clinicians must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies.

Four Criteria To Meet When Completing an SRA

It is acceptable for the SRA to be conducted or reviewed outside the performance period, but the analysis must:

- 1) Be unique for each performance period,
 - 2) Include the full MIPS performance period,
 - 3) Be conducted within the current calendar year.
 - 4) Be completed when a 2015 Edition CEHRT is implemented or upon installation or upgrade to a new system.
-



Business Associates

Definition of a Business Associate as Updated by the Omnibus Rule

The Omnibus Rule amends the definition of a “business associate” to mean a person or entity that **creates, receives, maintains or transmits protected health information** to perform certain functions or activities on behalf of a covered entity.

Business associates cannot avoid regulatory liability or limit that liability by refusing to sign a Business Associate Agreement. In addition, business associates must ensure that any subcontractors who handle PHI also have a business associate agreement in place. A business associate agreement of a subcontractor is not required to be in place with the covered entity, only the business associate.



Keep a List of All Business Associates

Common Business Associates. **Vendors who routinely access PHI i.e. vendor that gets authorizations**, IT Vendor, Answering Service, Billing Company, Clearinghouse, Transcription Service, Off-Site Record Storage & Retrieval, Record Disposal Service, Shredding Company, Marketing Companies, Consultants, Practice Management Vendors, Electronic Medical Record Software Vendor, Equipment Maintenance & Repair, IT Hardware Vendors, Courier Service, Lawyers, Copier Company, Translation Services, Collection Agencies and others who have access to your ePHI or computer network.

Not Business Associates: Cleaning staff, lawyers and accountants that do not receive patient information (PHI).

STEP 2 - Business Associates



OCR Business Associate Requested Information

Business Associate:					
Type of Service Provided	Choose an item.				
Web Site URL					
Point of Contact #1	First Name		Last Name		
Title					
Address					
City			State		Zip
Phone		Ext.		Fax	
Email					
Point of Contact #2	First Name		Last Name		
Title					
Address					
City			State		Zip
Phone		Ext.		Fax	
Email					
Business Associate Agreement in Place:	<input type="checkbox"/>		Date:	Click here to enter a date.	
Date of most recent Due Diligence:	Click here to enter a date.				
Type of Due Diligence Performed:	Choose an item.				
Compliance Verified by:					
Access Required:	Choose an item.	Other: List:			
Notes On Business Associate:	Click here to enter text.				



STEP 2 – Business Associates



Business Associate Agreements Are Required

Due Diligence – Are You Giving PHI to a Non-Compliant BA

Oversight – How are you Maintaining Oversight of PHI by the BA



STEP 2 - Business Associates



It is a HIPAA violation,
“Impermissible Disclosure” (BREACH)
for a Covered Entity to have a Business
Associate without a Business Associate
Agreement.

Do Not Give PHI Until the Agreement is Signed

Average Fine For No BAA - \$1,800,000





Beware Business Associate Agreements

Authorized Use of De-Identified Information. In addition to those uses described in Section 2.1 above, Business Associate may de-identify any and all PHI received or created by Business Associate under this Agreement, which de-identified information shall not be subject to this Agreement and may be used and disclosed on Business Associate's own behalf, all in accordance with the de-identification requirements of the Privacy Rule. Business Associate may aggregate, manipulate, use, disclose, sell, publish and distribute such de-identified health information and data provided that such de-identification is in accordance with HIPAA.



Beware Business Associate Agreements

1. Reporting of Unauthorized Uses or Disclosures of PHI and Breaches of Unsecured PHI.
 - (a) Business Associate shall report within a **commercially reasonable time** to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware.

STEP 2 – Business Associates

You Must Assess The Risk Posed By Each Business Associate



Vendor Management (Due Diligence of Vendors)

Lesson Learned: Virtua Medical Group

Breach by Business Associate Best Medical Transcription

Breach of 1, 654 individuals records.

Best Medical Transcription Misconfigured their Web Server allowing non-password protected access. Even though they uncovered the misconfiguration and corrected the error, Google retained cached indexes of patient files that remained publically accessible.

STEP 2 – Business Associates

You Must Assess The Risk Posed By Each Business Associate



Lesson Learned: Virtua Medical Group

A patient discovered their records on the internet and an investigation by the State of New Jersey.

Best Medical Transcription had a BAA with Virtua that required notification of security events (breaches) within 20 days.

Best Transcription never notified Virtua of the security incident.



You Must Access The Risk Posed By Each Business Associate

Lesson Learned: Virtua Medical Group

Result:

New Jersey's Attorney General fined Virtua Medical Group \$418,000.

Findings by State AG:

Failed to conduct and accurate and through risk assessment;
Failure to implement security measures to reduce risks; and
Failure to implement a workforce security training program.

“The medical practice’s duty to safeguard patient data also extends to managing risks posed by vendors.”

STEP 2 – Business Associates

You Must Assess The Risk Posed By Each Business Associate



OCR has noted that especially for new or smaller, non-established vendors, Covered Entities may need to perform additional measures of due diligence to ensure they are up-to-date with HIPAA Security measures and that they are aware of breach and security incident reporting requirements.

HITECH Associates recommends that you get 3rd Party Verification of HIPAA compliance by your vendors with significant access or storage of your PHI.

STEP 2 – Business Associates

Advanced Care Hospitalists



\$500,000 Settlement for no Business Associate Agreement

Advanced Care Hospitalists of Lakeland engaged Doctor's First Billing Services to perform billing for the group. The OCR determined that no Business Associate Agreement was in place. Doctor's First Billing placed approximately 9,000 patient records on their web site with no password protection or other security measures in place.

Besides the \$500,000 settlement, ACH also agreed to enter into a two-year corrective action plan.



Cloud Computing

Service Level Agreement or BAA should include:

No “Information Blocking”

Availability

Backup – Disaster Recovery

Security Controls

Accounting of Disclosures

Return or Destroy

STEP 2 - Business Associates



Cloud EHR

**You Do Not Have A
Backup Of Your
Patient Records**



Policies and Procedures

Privacy Rule –

Patient's Rights
Minimum Necessary
Update for Information Blocking

Security Rule –

Risk Assessment
IT Security Controls
Sanctions

Privacy Rule

Patient's Privacy Rights

1. Right to Access.
2. Right to Request to Amend.
3. Right to Confidential Communications.
4. Right to Accounting of Disclosures.
5. Right to Restrict Information.
6. Right to Restrict Information to Health Plan.
7. Right to Receive Notice of Privacy Practices.
(Patients must resign Acknowledgement every 3 years)
Right to File A Complaint.

Most Common Reason for OCR Investigation – Privacy Right Violated.

MINIMUM NECESSARY Standard

The **Minimum Necessary Standard**, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. **The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.** The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.



STEP 3 – Policies & Procedures

HIPAA Security Rule

The Security Matrix



6 Basics of Risk Analysis and Risk Management

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)	(A)
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedures (A)
		Termination Procedures (R)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions (A)
		Access Authorization and Modification (A)
		Security Reminders (A)
		Protection from Malicious Software (A)
Security Awareness and Training	§ 164.308(a)(5)	Log-in Monitoring (A)
		Password Management (R)
		Response and Reporting (R)
Security Incident Procedures	§ 164.308(a)(6)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedures (A)
		Applications and Data Criticality Analysis (A)
Contingency Plan	§ 164.308(a)(7)	
Evaluation	§ 164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement (R)

CMS

6 Basics of Risk Analysis and Risk Management

PHYSICAL SAFEGUARDS

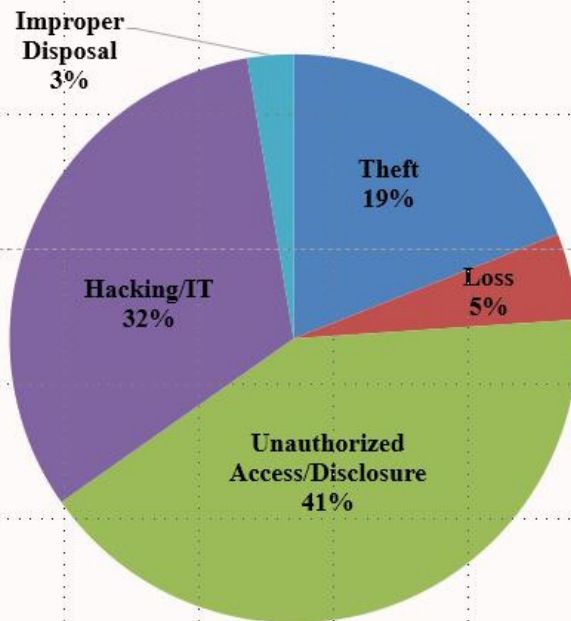
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	§ 164.310(b)	
Workstation Security	§ 164.310(c)	(R)
Device and Media Controls	§ 164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
TECHNICAL SAFEGUARDS		
Access Control	§ 164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (A)
		Automatic Logoff 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)	Integrity Controls (A)
		Encryption (A)
Transmission Security	§ 164.312(e)(1)	
ORGANIZATIONAL REQUIREMENTS		
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)

CMS

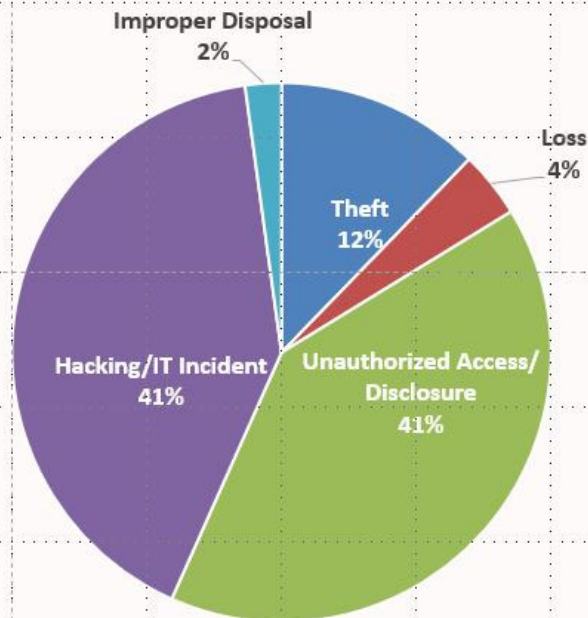




500+ Breaches by Type of Breach



Oct 1, 2015 through Sep 30, 2018



Jan 1, 2018 through Sep 30, 2018

**Insider
Threat**

Reasonable Security



NOT PERFECT SECURITY

Looking for Known Vulnerabilities

Reasonable & Appropriate Safeguards



Reasonable Security

Scalable and Flexible



Risk Based – Not Compliance Driven

Be Able To Adapt To New Threats

Access Risks Around PHI Storage

Strategic Planning is Critical

Budgeting For Security



REASONABLE & APPROPRIATE SECURITY FOR HIPAA COVERED ENTITIES & BUSINESS ASSOCIATES

There is no such thing as
Perfect Security

BALANCE

Cost vs. Productivity

There is a minimum standard of care that needs to be implemented.

You should be implementing the HIPAA “Safe Harbor”.

Question

Does your organization spend more on coffee every year than security?

You Need to

Aggressively Protect PHI

A Little Healthy Paranoia promotes a “culture of preparedness”.

Healthy paranoia is dealing with life realities in an optimistic way,
and not closing your eyes to reality.

All Computers Should Be Using Windows 10 Pro

Reasonable and Appropriate Security Measures

Firewall	Complex Passwords	Backups of PHI	Hardening
Anti-Virus	Physical Security	WiFi Security	Mobile Devices
Anti-Malware	Risk Assessment	SPAM Filtering	Policies
Patching	Risk Management Plan	Remote Access Security	Audit Reviews
Encryption	Network Configurations	Monitored Network	Staff Training
Email	Business Associate Management	Vulnerability Scans	External Vulnerability Scanning

Firewall

Question: Are you using the firewall supplied on the router you received from your internet company?

Firewall

A firewall is a [network](#) security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.

A firewall acts as a barrier between a trusted network and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied.

Your Primary Protection From the Outside World

Firewall

Question: When was the last time your IT vendor/staff updated the firmware/software?

Firewall

The Router/Firewall provided by your Internet Provider does not meet the requirements under HIPAA. These Router/Firewalls are residential grade and have numerous known vulnerabilities which allow cyber criminals easy access to your network.



Firewall

Firewall Software Security	
Gateway Anti-Virus	Spamblocker
URL Filtering	DLP – Data Loss Prevention
Network Discovery	Reporting Tools
Application Control	Control Console
IDPS – Intrusion Detection and Prevention System	
APT – Advanced Malware Protection	

Firewall

**Firewalls
Must Be
Updated**

**Firewalls
Need to be
Configured
by a
Professional**

**Regular
External
Scans
Should be
Performed**

Firewall

Reasonable Security
WHAT YOU NEED TO KNOW



SonicWall TZ300 Promotional Tradeup With 3YR AGSS

The 3 & Free Tradeup Promo from SonicWall gets you a FREE SonicWall TZ300 appliance with the purchase of 3-Year Advanced Gateway Security Suite. Additional discounts are available when you pair your promo with our Configuration Service. Get a quote today.

Regular Price: ~~\$1,378.00~~

Special Price \$1,102.00

[Add to Cart](#)



SONICWALL



[Compare](#)

SonicWALL TZ600 TotalSecure (1 Year)

- » Maximum Speed: **1500 Mbps**
- » UTM Speed: **500 Mbps**
- » Maximum VPN Speed: **1,100 Mbps**
- » Concurrent Connections: **150,000**
- » Site-to-Site VPN Tunnels: **50**
- » Bundled Global VPN Client Licenses: **2 (25 Available)**
- » SSL VPN licenses: **2 (200 Available)**
- » Wireless Controller: 802.11 A/B/G/N Wireless LAN
- » Bundled with: **(1) Year gateway antivirus, content filtering, spyware protection, intrusion prevention and 24x7 technical support.**

Yearly Renewal Starts at: \$839.00. [View All Renewals](#)

[▶ Video Overview](#) [▶ Online Demo](#) [▶ Datasheet](#) [▶ More Information](#)

Regular Price: ~~\$2,465.00~~

Special Price \$1,972.00

[Add to Cart](#)

[Request a Quote](#)

[Shipping Cost](#)

Availability : Ships Monday



Anti-Virus

Computer crime

Vulnerability

Eavesdropping

Malware

Spyware

Ransomware

Bootkits

Keyloggers

Screen scrapers

Exploits

Backdoors

Logic bombs

Trojans

Viruses

Worms

Rootkits

Payloads

Denial of service

Anti-Virus

Antivirus or **anti-virus** software (**AV**), sometimes known as **anti-malware** software, is [computer software](#) used to prevent, detect and remove [malicious software](#).

Anti-Virus and Anti-Malware

Norton	McAfee	Web Root	Bit Defender
Kaspersky	Security Essentials	Windows Defender	Bit Defender
Avast	Eset	Trend Micro	F-Secure
Vipre	Avira	AVG	Intego
Panda	Malware Bytes Pro	Malware Bytes	BullGuard

Anti-Virus

The cost of Commercial Grade Anti-Virus & Anti-Malware Software

Approximately \$15 to \$20 per computer per year.

Patching

A **patch** is a piece of software designed to update a [computer program](#) or its supporting data, to fix or improve it.^[1] This includes fixing [security vulnerabilities](#)^[1] and other [bugs](#), with such patches usually called **bugfixes** or **bug fixes**,^[2] and improving the [usability](#) or [performance](#).

Patching

Reasonable Security

Software
Requiring
Patching

Microsoft Windows	Apple OS
Adobe	Microsoft Office
Java	All Internet Browsers
Electronic Medical Records	Practice Management

Patching

Performed By IT

Automatic Patching

Software or Manual

Patching

Reasonable Security
Costs of Patching

IT Vendor: \$125 to \$250 per Hour

**Automatic: Free but must be checked and not available on all software.
Windows has automatic updates.**

Software Products: \$10 to \$60 per computer per year.

Patching

Vulnerability Scanning

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weak points or poorly constructed parts.

Backup

1. DATA BACKUP PLAN (R) - § 164.308(a)(7)(ii)(A)

The Data Backup Plan implementation specification requires covered entities to:

“Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”

Most covered entities may have backup procedures as part of current business practices. Data Backup plans are an important safeguard for all covered entities, and a required implementation specification.

Reasonable Security
Required

Backup

Ransomware Protection

Have Air-Gapped, non connected backup.



Backup

On-Site Backup

Fastest Restoration of Data

Make sure all PHI is backed up.

Patient accounting systems, electronic medical records, health maintenance and case management information, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used.

Backup

On-Site Backup

- **Frequency of Backup**
Recommended : Hourly
- **Encryption**
- **Segmented / Air Gapped**

Off-Site Backup

- **BAA Agreement with Service Level Agreement Required**
-

Monitored Network

Reasonable Security Considerations

Under the HIPAA Security Rule, covered entities and business associates have an obligation to have policies and procedures in place to prevent, **detect**, contain and correct security violations. 45 CFR 164.308(a)(1)(i). The regulations also require covered entities and business associates to “Implement procedures to **regularly** review records of information security system activity, such as audit logs, access reports and security incident tracking reports.” 45 CFR 164.308(a)(1)(ii)(D) It also requires the covered entity to implement hardware, software and/or procedural processes that **record and examine** activity in information systems containing electronic protected health information (ePHI). 45 CFR 164.312(b)

Monitored Networks Reveal Network Intrusions Faster To Reduce Potential Harm to Your Organization.

Encryption

Reasonable Security
ADDRESSABLE

ENCRYPTION AND DECRYPTION (A) - § 164.312(a)(2)(iv)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity must:

“Implement a mechanism to encrypt and decrypt electronic protected health information.”

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (i.e., type of procedure or formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (i.e., translate) the text and convert it into plain, comprehensible text.

There are many different encryption methods and technologies to protect data from being accessed and viewed by unauthorized users.

Reasonable Security
BOTTOM LINE

Encryption

ENCRYPTION is a
“SAFE HARBOR”

It is recommended that all laptops be encrypted.



WiFi Security

WPA2 – Ten Digit Passcode Encrypts your transmission.

MAC Address Filtering adds a second layer of authentication.

SSID Broadcasting – Disable to hide your network.

WIPS - a **wireless intrusion** prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (**intrusion detection**), and can automatically take countermeasures (**intrusion prevention**).

REMOTE ACCESS

Reasonable Security
METHODS

Data in Motion

Data in motion refers to data going through networks. Encrypting data in motion is straightforward: Valid encryption processes must “comply with the requirements of Federal Information Processing Standards (FIPS) 140–2.” While there are many technical requirements involved, finding a vendor that offer products that are FIPS 140-2 compliant, is the solution.

Remote Desktop Protocol (RDP) is a major access for Cybercriminals.

REMOTE ACCESS

Reasonable Security
SECURITY

Secure Your Remote Access

Data Encryption

Multi Factor Authentication (MFA)

Restrict Access Rights

Audit, Audit, Audit – especially BAs with Remote Access



58:59

1 file will be deleted.

JIGSAW RANSOMWARE

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.

Thank you

 Spyware.com

Ransomware or Any Network Intrusion:

A Breach of Confidentiality, Integrity and Availability is Presumed.



Breach Risk Assessment to Perform LoProCo.

Low Probability that the PHI has been compromised.

Confidentiality – has PHI been accessed?

Integrity – most strains of ransomware copy files to encrypted container.

Availability – Loss of access to your PHI

Ransomware Is A Breach of PHI



Burden of Proof

A Breach Risk Assessment Must Be Performed.

Has your data been exfiltrated?

Forensic IT may be required to make this determination.

ClientName

Person Making Report: [Click here to enter text.](#)

Breach Reported By: **Workforce Member of Organization**

Date Breach Known or Suspected: [Click here to enter a date.](#)

Date the Breach Occurred (If Known): [Click here to enter a date.](#)

Case Number Assigned (Optional): [Click here to enter text.](#)

Under the final rule, **breach** is defined as "an acquisition, access, use, or disclosure of protected health information in a manner not permitted...and) is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised (emphasis added)." According to HHS, "breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised."

Mark all types of PHI that were involved: Paper PHI Electronic PHI Sensitive PHI Verbal PHI

Number of records involved in breach: [Click here to enter text.](#)

RISK ASSESSMENT

1. What was the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification? *Could this information be used by an unauthorized recipient to further his own interests? Could it be re-identified relatively easily? Would it facilitate identity theft (SSN, credit card #, etc.)?*

Identifiers:

Sex	Marital Status	M	First Initial	L	Full Address	Social Security Number	M	DOB - last 4	D
At Risk Member	Health Plan Member	Active Member	IF	Full/Partial Name	Service Street/Box	Y	Y/N	Y	
Children	Business Associate	Full Name	F	Work/Residence	Alt	Alt/Postal/Phone	F	State	N
Medical Records	Other	Click here to enter text.							

Payment or Treatment Information:

1. **Payment:** [Click here to enter text.](#)

2. **Healthcare Operation:** [Click here to enter text.](#)

2. Who was unauthorized person who used the protected health information or to whom the disclosure was made? *(Is the recipient already obligated to protect PHI? Is recipient trustworthy? Identification also helps as mitigation—the recipient is already on the radar if the data is later misused.)*

Organization/Person/Staff Member Involved: Choose an item.

Name of Person: [Click here to enter text.](#) HIPAA Covered Entity?

3. Was the protected health information actually acquired or viewed? *Recovery of a lost laptop with PHI would present potential compromise. If forensic analysis shows the laptop was not accessed since prior to its loss, there is no actual compromise. PHI listed in an individual email present on actual compromise. If recipient claims it didn't read it, the weight that is given is immaterial and based on the trustworthiness of the individual (B2).*

Answer: **Yes**

Describe nature of review: Choose an item.

4. To what extent has the risk to the protected health information been mitigated? *Recipient makes document not subject to disclosure. A note of disclosure and/or a Non-Disclosure Agreement may prove useful as mitigating factors. Encryption as mitigation—YES! Must meet most encryption standards. There is no "crypton-equivalent" available for paper documents.*

List: Choose an item.

List Additional Mitigation: [Click here to enter text.](#)

List any attachments: **(copy of PHI data, letters, depositions, attestations)**

[Click here to enter text.](#)

Privacy Security breach incident Report © 2015 HITRUST Compliance Associates. All Rights Reserved. Page: 1



Ransomware Is A Breach of PHI



ClientName

Person Making Report: [Click here to enter text.](#)

Breach Reported By: **Workforce Member of Organization**

Date Breach Known or Suspected: [Click here to enter a date.](#)

Date the Breach Occurred (If Known): [Click here to enter a date.](#)

Case Number Assigned (Optional): [Click here to enter text.](#)

BREACH
Security Risk Assessment
& LoProCo Determination

Under the final rule, **breach** is defined as "an acquisition, access, use, or disclosure of protected health information in a manner not permitted...[and] is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised (emphasis added)." According to HHS, "breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised."

Mark all types of PHI was involved: Paper PHI Electronic PHI Sensitive PHI Verbal PHI
 Number of records involved in breach: [Click here to enter text.](#)

RISK ASSESSMENT

1. What was the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification: (Could this information be used by an unauthorized recipient to further his own interests? Could it be re-identified relatively easily? Would it facilitate identity theft (SSN, credit card #, etc.)?)

Identifiers:	Date of Birth	Sex	Race	Ethnicity	Height	Weight	Hair Color	Eye Color	Complexion	Scars	Other
Account Number	Health Plan Number	Account Number	Card/ID/Reference	Online Identifier	URLs						
IP Address	Network Location	File Name/Name	Device/Manufacturer	Device/Manufacturer	Device						
Medical Record #	Click here to enter text.										

Payment or Treatment Information:

Treatment	Click here to enter text.
Payment	Click here to enter text.
Healthcare Operations	Click here to enter text.

2. Who was unauthorized person who used the protected health information or to whom the disclosure was made: (Is the recipient already obligated to protect PHI? Is recipient trustworthy? Identification also helps as mitigation—the recipient is already on the radar if the data is later misused.)

Organization/Person/Staff Member Involved: Choose an item.

Name of Person: [Click here to enter text.](#) HIPAA Covered Entity?

3. Was the protected health information actually acquired or viewed: (Recovery of a lost laptop with PHI would present potential compromise. If forensic analysis shows the laptop was not accessed since prior to its loss, there is no actual compromise. PHI found to an individual would present an actual compromise. If recipient claims "I didn't read it," the weight that is given in consideration will depend on the involuntariness of the individual (R2).)

Answer: **Yes**
 Describe nature of review: Choose an item.

4. To what extent has the risk to the protected health information been mitigated: (recipient returns document and states he did not view it. A letter of attestation and/or a Non-Disclosure Agreement may prove useful as mitigating factors. Encryption as mitigation—YES! Must meet encryption standards. There is no "encryption-equivalent" available for paper documents.)

List: Choose an item.
 List Additional Mitigation: [Click here to enter text.](#)
 List any attachments: (copy of PHI data, letters, depositions, attestations)
[Click here to enter text.](#)

Privacy Security Breach Incident Report © 2015HITECH Compliance Associates. All Rights Reserved. Page 1

A Breach Risk Assessment Must Be Performed.

Forensic Review Items to document:

- ✓ Variant of the Ransomware
- ✓ Number of Patient Records Affected
- ✓ **Network Activity**
- ✓ Did the Malware Communicate with the Attacker
- ✓ Number of Days In the System
- ✓ A Network Activity Review
- ✓ Review for Other Malware such as Backdoors
- ✓ Data Integrity Checks
- ✓ Reasonable Security Measures in Place
- ✓ Boot Drive Locked or Files Locked
- ✓ Backdoors or Other Malware Present



Ransomware:

The Stakes Are Higher, Pay or We Will Release Your Patient's Information Onto the Internet

COMPLIANCE
REGULATIONS
GUIDELINES



TAMPA – The Tampa Bay Surgery Center sent a letter to 25,000 patients alerting them that their personal information was stolen last month and posted on a Twitter account used by the hacker group “The Dark Overlord.”

The Dark Overlord Gang stated in a press release that “Tampa Bay Surgery Center annoyed us” and that was the reason for the posting of PII.



HIPAA Training

- Yearly to Your Policies and Procedures
General Training is not Sufficient.
- Before Access is Given to PHI
- Updates Throughout the Year.
- Document



Training and Awareness are Keys

to our practice preventing a successful cybercrime attack. Even with security measures such as our firewall, anti-virus and other network protections, your actions can expose our systems to ransomware and other malicious software. It is the policy of our practice to ensure all workforce members are properly trained on how to avoid malicious software. As an added benefit, these same precautions will aid you protect your files and information from being access or encrypted, so always practice these safety measures when using the internet.



Email Attachments
Web Site Browsing
Social Engineering



HIPAA Training

Training to Your Policies and Procedures

Training on Healthcare Cybersecurity

**91% of cyberattacks begin with
a spear phishing email**

**89% of phishing attacks are orchestrated
by professional organized crime**

This Is A Ransomware Email That Has Made Cybercriminals Millions of Dollars

Think Before You Click!



Training and Awareness are Key

Problem with parcel shipping, ID:00000102090

FedEx Ground <arnold.montgomery@giani-media.com> **1**

Sent: Wed 10/5/2016 3:49 AM

To: mm@hipaacompliancekit.com **2**

Message **3** FedEx_00000102090.zip (5 KB) **3**

Dear Customer, **4**

We could not deliver your item.
Shipment Label is attached to email.

Yours sincerely, **5**
Arnold Montgomery, **6**
FedEx Operation Manager. **7**

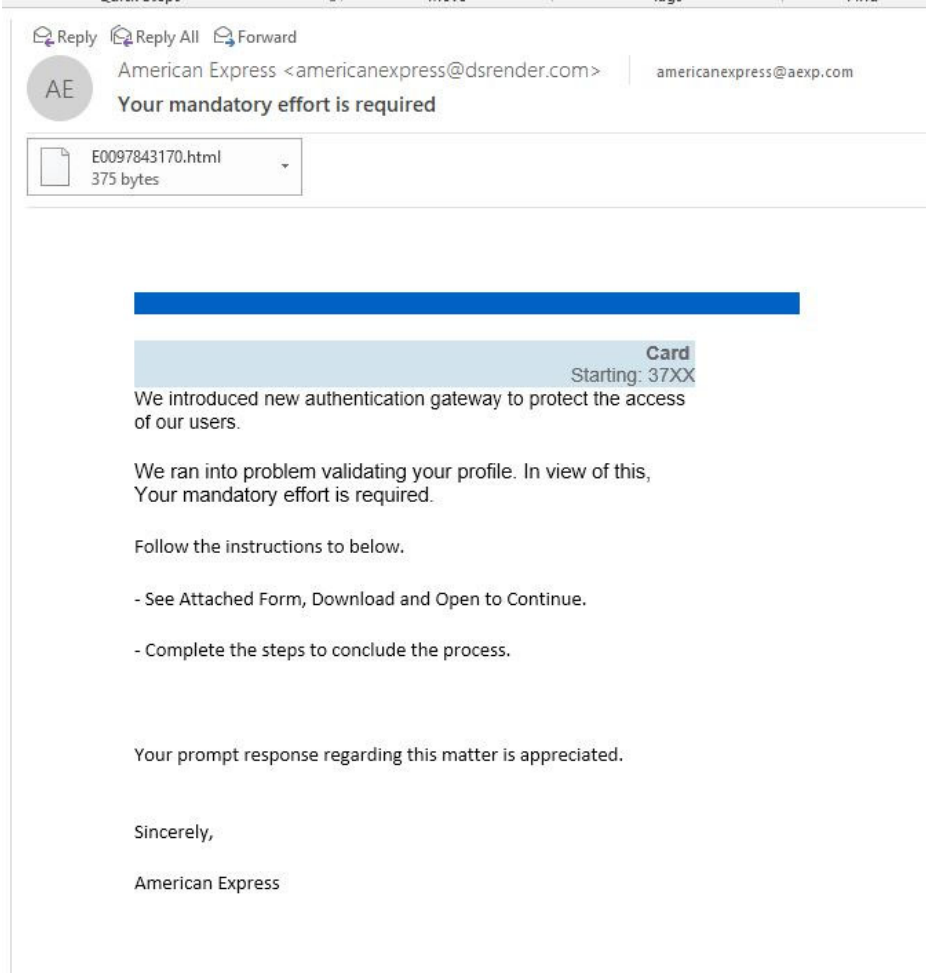
Review All Emails Containing Attachments

- 1** Look at the return email address, does it match the Business Name?
- 2** How did the sender get my email address?
- 3** Never open a .zip file contained as an attachment in an email.
- 4** They have my email address, but do not know my name or Company Name!
- 5** This is a common greeting on phishing attacks coming from outside the U.S.
- 6** A comma after the name is not how most of us sign an email.
- 7** Note Operation, not Operations Manager and the period at the end.

STEP 4 – HIPAA Training

Cybersecurity Training

Malicious Email




STEP 4 – HIPAA Training

Verizon Email

 Reply  Reply All  Forward

 N notifications2@verizon.com <ventas@gasq.com.mx> | mm@HipaaComplianceKit.com

Invoice eMail - 02-05-2019

 Follow up. Start by Tuesday, February 5, 2019. Due by Tuesday, February 5, 2019.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

For the account(s) noted below, Verizon invoice(s) are now available to view online via the Verizon Enterprise Center:

Billing Acct. No.
2021614837674

<https://enterprisecenter.verizon.com/enterprisesolutions/global/dlink/ncas/PdfBillView.do?MAN=2021614837674&BAN=2021614837674&OSID=79&BILLDATE=2019-02-05>

You can also click on the billing account number hyper link for each invoice and get directly to the DOC copy of the invoice from Verizon Enterprise Center.

Please do not reply to this e-mail message.

Your Verizon Team



If you have received this notification in error, or if you need further assistance accessing your invoice, please contact Verizon Enterprise Center Support at (800) 286-4744.



Bank of America



Reply Reply All Forward



Bankofamerica Business <grupopharma@grpharma.com.ec>

mm@HipaaComplianceKit.com

Your Bankofamerica, N.A. Account Has Been Suspended



Please contact Member Services to re-activate your suspended account.

This email was sent to mm@HipaaComplianceKit.com as part of Bankofamerica, N.A..
If you have received this email in error, please send an e-mail to eBanking@Bankofamerica.com.



HIPAA Training

Importance of Complex Passwords

Password Spraying – a Brute Force attack.

Attacker uses a single password against many accounts.

Most common targets: Cloud services and Email Applications

A list of the top – 1000 passwords is effective 75% of the time, according to the U.K.'s National Cyber Security.

Password Managers help you maintain complex passwords.

Hacker Forum – a dark web site has 773 million email addresses and 21 million passwords for sale.

STEP 4 – HIPAA Training

HIPAA Training

Importance of Changing Passwords Routinely

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

mccoy.tampa@gmail.com | pwned?

Oh no — pwned!

Pwned on 7 breached sites and found no pastes ([subscribe](#) to search sensitive breaches)

 3 Steps to better security

[Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

STEP 4 – HIPAA Training

HIPAA Training



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses



ShareThis: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Names, Passwords



Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses



HIPAA Training

Common Social Engineering Deception Methods:

Authority
Likability
Reciprocation
Consistency
Validation
Scarcity

Authority – People will tend to obey authority figures, even if they are asked to perform objectionable acts.

Liking – People are easily persuaded by other people whom they like.

Reciprocity – People tend to return a favor, thus the pervasiveness of free samples in marketing.

Commitment and consistency – If people commit, orally or in writing, to an idea or goal, they are more likely to honor that commitment because they have stated that that idea or goal fits their self-image.

Validation – People will do things that they see other people are doing.

Scarcity – Perceived scarcity will generate demand. For example, saying offers are available for a "limited time only" encourages sales.

Wikipedia



Breach Notification Rule

Staff Need to be Able to Identify Breach

Breach Security Risk Assessment Must be Performed

Suspected Breach is Actual Breach.

Breach Reporting to OCR Portal (at end of year)

Small Breaches

500 or More - Immediately





Breach Notification Plan

Plan In Place for Breaches of Under 500 Records.

Plan In Place for Breaches of 500 or More Records.

HIPAA Breaches Must Be Reported to the Patient

State Laws May Increase Your Breach Notification Requirements

Breach Costs can be Staggering Even without Fines.
Determining if a Breach Occurred Can Cost Thousands.



Security Incident Planning



Identify, Protect, Detect, Response and Recover

Identify Assets that Require Protection

Ensure Safeguards/Controls In Place

Review Techniques Used To Detect Incidents

Have Mitigation Plans – Respond to Incident

Test Recover Methods



STEP 5 – Breach Notification

Security Incident Plan Is Required by HIPAA

Focus On Recovery



Security Incident Response Plan			
Organization			
HIPAA Compliance Officer	Click here to enter text.	Phone #	Click here to enter text.
Email Address	Click here to enter text.		
Date of Incident Report	Enter Date	Date Incident Known	Enter Date
Incident Response Team Members			
Team Member		Title	
Team Member		Title	
Team Member		Title	
<small>Security Incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 C.F.R. 164.304.</small>			
Incident Response Objectives			
❖ Preserve Data			
❖ Investigate the behavior of the malware/incident			
❖ Determine if PHI was exfiltrated or compromised			
❖ Prevention			
❖ Quick Recovery and Return to "Normal" Operations			
Purpose and Objectives of Policy			
▪ Ensure All Events and Responses Are Documented in Detail			
▪ Realization that not all incidents can be prevented.			
▪ Make It More Difficult for Malicious Actors To Infiltrate Our Network			
▪ Determine hardware/software/policies required to prevent & detect if Protected Health Information (PHI) has been "Compromised"			
Statement of Management Commitment			
The Management Team is strongly committed to the ongoing maintenance, network security and remediation of security events required to protect the PHI, our computer network and Protected Health Information.			
Incident Response Ransomware			
Robust security incident procedures for responding to a ransomware attack should include processes to:			
▪ detect and conduct an initial analysis of the ransomware;			
▪ contain the impact and propagation of the ransomware;			
▪ eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;			
▪ recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and			
▪ conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.			
1 Page Security Incident Policy – HIPAA Compliance Kit			

Attachments

Software Inventory

Hardware Inventory

Security Incident Report



Contingency Plan



Backup of All PHI

Off-Site Backup Required

Image Backup Should Be Reviewed
Proper Segmentation

Tested and Evaluated Yearly





DOCUMENTATION

If's It's Not Documented, It's Not Done.



Documentation



Documentation is Key to Proving HIPAA Compliance

Mobile Device Policy

Patient Forms to Invoke their HIPAA Rights

Letters to Respond to HIPAA Requests

Certification of Proper Disposal of Systems Containing PHI

Job Descriptions

Visitor Sign-In Sheets

**All HIPAA documentation
must be kept for a period of
6 years.**



Authorization Forms – Elements Required

Authorization Form Medical Records Release Form Nine Elements Required by HIPAA



AUTHORIZATION TO USE AND/OR DISCLOSE MEDICAL RECORDS I give authorization to the provider listed below to disclose a copy of the specific health/medical information identified below:

NAME OF PATIENT		SS#
TO: (Name, Address, Phone of Recipient of Records)		
Name		Phone
Address		
City/State	Zip	
RECORDS FROM (Who is Releasing the Records):		
Name		Phone
Address		
City/State	Zip	
For the Following Purposes:		
<input type="checkbox"/> Continued Medical Care	<input type="checkbox"/> Personal Information	<input type="checkbox"/> Legal Follow-up
<input type="checkbox"/> Disability Insurance	<input type="checkbox"/> Other:	
By Checking the Boxes Below, I Specifically Authorize the Use and/or Disclosure of the Following Health Information And/or Medical Records, if Such Information And/or Records Exist:		
<input type="checkbox"/> Please send the entire Medical Record (all information) to the above named recipient.		
<input type="checkbox"/> Office Notes and Reports	<input type="checkbox"/> Most recent one-year history	<input type="checkbox"/> Most recent three-year history
<input type="checkbox"/> Rx History	<input type="checkbox"/> Transcribed hospital reports	<input type="checkbox"/> Laboratory reports
<input type="checkbox"/> Billing Statements	<input type="checkbox"/> Diagnostic Reports	<input type="checkbox"/> Diagnostic Films
<input type="checkbox"/> Others Listed Here:		
The Following Items Must Be Initialed to Be Included in the Use And/or Disclosure:		
<input type="checkbox"/>	HIV/AIDS relate information and/or records HBV, TB or Other Communicable Diseases	
<input type="checkbox"/>	Mental Health Information and/or Records	
<input type="checkbox"/>	Domestic Violence	
<input type="checkbox"/>	Genetic Testing Information and/or records	
<input type="checkbox"/>	Drug/Alcohol diagnosis, treatment or referral information (Federal regulations require a description of how much and what kind of information is to be disclosed.) Describe:	
<input type="checkbox"/>		

a description of the information to be used or disclosed.

a description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization.

name or other specific identification of the persons or class of person(s) authorized to make the requested use or disclosure.

name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure.

an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

state that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Rule.

the signature of the individual and a date.

notify the individual of the right to revoke the authorization and the process for so doing. Notify the individual that a revocation will not effect action already taken in reliance on the authorization form.

notify the patient that a provider may not condition treatment on the patient signing the authorization form. (Please note: different rules apply if the use or disclosure is for research-related treatment or PHI created for use by a third party.)

See HIPAA Essentials: Page 21 for a list of required elements.

Subpoenas



Must Have Signed Valid Authorization

Or

Notice of Production (HIPAA Release)

HIPAA does not allow release of PHI with only a Subpoena



Subpoenas



After eleven years of litigation, including two decisions by the Connecticut Supreme Court, *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.* has finally reached a verdict. Last month, the jury awarded the plaintiff **\$853,000 in damages** in connection with her physician practice's 2005 release of medical records in response to a **non-HIPAA compliant subpoena**. **In addition: the practice violated its notice of privacy practices, which stated it would only release medical records with a patient authorization or as otherwise required by law.**

The second Supreme Court ruling, as a case of first impression in Connecticut, held that a cause of action exists in Connecticut when a physician breaches his or her duty of confidentiality established by virtue of the physician-patient relationship.

STEP 8 – System Activity Review

System Activity Review (User Audit Log)



User Audit Logs Must Be Reviewed & Documented

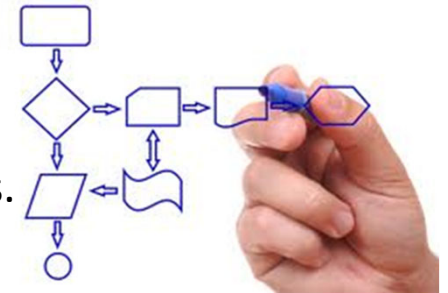
Use and Disclosure Tracked = Fax Machine, Firewall Penetration Reports, etc...

Monthly Activity

Your HIPAA Homework

Looking for Unusual or Suspicious Activity

May be the only way to detect an Insider Threat, Hacking and/or Other Improper Access and Use of Patient Records.



STEP 8 – System Activity Review

User Audit Log

Patient Name : Shannen Curran						
2009-02-01	9120	CC	viewed	Sam Willis	2012-11-14 07:18:34	127.0.0.1
2009-02-01	9120	CC	modified	Sam Willis	2012-11-14 07:18:50	127.0.0.1
3 month f/u Headache abdominal pain						
Patient Name : Jeff Curran						
2012-12-06	9118	CC	viewed	Sam Willis	2012-12-06 10:03:18	192.168.10.108
2012-12-06	9118	CC	viewed	Sam Willis	2012-12-18 16:12:12	192.168.1.219
Patient Name : Shannen Curran						
2009-02-01	9120	CurrentMedication	viewed	Sam Willis	2012-11-14 07:18:34	127.0.0.1
2009-02-01	9120	CurrentMedication	modified	Sam Willis	2012-11-14 07:18:51	127.0.0.1
<i>CurrentMedication:</i>						
Tylenol: , Size: 325 MG, Formulation: Tablet, Take: 1 tablet as needed, Route: Orally, Frequency: every 6 hrs, Duration: , Amount: , Refills: , Auth No: Minocycline HCl: , Size: 100 MG, Formulation: Capsule, Take: 1 capsule, Route: Orally, Frequency: every 12 hrs, Duration: 14 day(s), Amount: 28, Refills: , Auth No: Differin: , Size: 0.3 %, Formulation: Gel, Take: 1 application to affected area at bedtime, Route: Externally, Frequency: Once a day, Duration: , Amount: , Refills: , Auth No: Percocet 5-325 mg 30: , Size: 5-325 mg, Formulation: Tablets, Take: one or two tablets, Route: orally, Frequency: every four to six hours prn pain, Duration: , Amount: 30, Refills: No, Auth No: OxyContin: , Size: 20 MG, Formulation: Tablet Extended Release 12 Hour, Take: as directed, Route: Orally, Frequency: , Duration: , Amount: , Refills: , Auth No:						
Patient Name : Jeff Curran						
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-06 09:18:25	192.168.10.108
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-06 10:03:18	192.168.10.108
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-18 15:28:20	192.168.1.219
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-18 15:32:41	192.168.1.219
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-18 16:12:12	192.168.1.219
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2012-12-18 16:16:37	192.168.1.219
2012-12-06	9118	CurrentMedication	viewed	Sam Willis	2013-01-10 15:20:41	192.168.1.113
Patient Name : Shannen Curran						
2009-02-01	9120	MedicalHistory	modified	Sam Willis	2012-11-14 07:18:50	127.0.0.1
MedicationFlag:Y						
Patient Name : Jeff Curran						
2012-12-06	9118	MedicalHistory	modified	Sam Willis	2012-12-06 08:38:25	192.168.10.108
NextAppt:6 Weeks NextApptOpt:0 NextApptReason: FollowUpNA:0						
Patient Name : Shannen Curran						
2009-02-01	9120	Allergies	viewed	Sam Willis	2012-11-14 07:33:38	127.0.0.1
2009-02-01	9120	Allergies	viewed	Sam Willis	2012-11-14 07:34:33	127.0.0.1
Patient Name : Jeff Curran						
2012-12-06	9118	Allergies	viewed	Sam Willis	2012-12-06 09:18:25	192.168.10.108
2012-12-06	9118	Allergies	viewed	Sam Willis	2012-12-18 15:28:19	192.168.1.219
2012-12-06	9118	Allergies	viewed	Sam Willis	2012-12-18 15:32:41	192.168.1.219
2012-12-06	9118	Allergies	viewed	Sam Willis	2012-12-18 16:16:37	192.168.1.219
2012-12-06	9118	Allergies	viewed	Sam Willis	2013-01-10 15:20:41	192.168.1.113
	9118	Vitals	viewed	Sam Willis	2012-08-23 15:19:39	10.201.100.65
	9118	Vitals	viewed	Sam Willis	2012-09-05 18:58:35	192.168.2.5
	9118	Vitals	viewed	Sam Willis	2012-09-05 19:00:41	192.168.2.5
	9118	Vitals	viewed	Sam Willis	2012-09-05 19:15:00	192.168.2.5

STEP 8 – System Activity Review

System Activity Review

Review Workforce Members for:
Number of Records Accessed
Location of Access
Time in Chart
Activity – Modified, downloaded, Viewed...

“HIPAA Homework”

Each Workforce Member Should Be Reviewed
Twice Per Year Minimum



Audit Log Management Report

My Medical Practice

HIPAA Security Officer: Michael McCoy

Beginning Period of Review: 2/1/2015

Ending Period of Review: 2/28/2015

Audit Logs Are Stored in System Audit Logs are Attached

PURPOSE: To protect against threats or hazards to the security of the information and to prepare for investigations on potential security breaches our organization reviews system audit logs on a routine bases. This report is the responsibility of the HIPAA Security Officer.

User Audit Logs Reviewed

USER ID 1	USER ID 2	USER ID 3
Gina123	Holly456	Kathy789
2/2/2015	2/10/2015	2/4/2015

Audited For: Viewed, Modified, Created, Time in Chart, Inappropriate Access, Access Same Last Name, Location of Access, Login Success/Failure

Patient Charts Reviewed

PATIENT ID 1	PATIENT ID 2	PATIENT ID 3
12345	23456	34567
2/13/2015	2/6/2015	2/17/2015

Audited For: Viewed, Modified, Created, Time in Chart, Inappropriate Access, Access Same Last Name, Location of Access, Login Success/Failure

Results of Audit Log Review

Findings this Period: The following items require investigation:

Investigations Required: Staff Member went through 2X number of patient records expected.
Staff member stated that another employee forgot their User ID and Password so they shared her User ID for the day. Verified that the other employee had no activity for the day and gave both employees a Group 1 Sanction.

All findings that require additional investigation will be documented with a Security Incident Report.

Reviewed By: Michael D. McCoy

Title: HIPAA Security Officer



System Activity Review

Log-in Success and Failures to the Network also need to be reviewed.

Review Server and Workstation Event Logs for unusual and/or suspicious activity.

Mobile Device Security & HIPAA

Encryption and keeping confidential information off laptops and cellphones are among the ways to prevent Mobile Device Breaches.

Before allowing Cell Phones and Tablet to be used by physicians and staff, make sure you have documented policies and procedures on their use and security requirements. This is best accomplished through a Mobile Device Policy signed by all workforce members, regardless of who owns the device.



Bring Your Own Device Policy/Organization Owned Device Policy

Organization: _____

HIPAA Compliance Officer: _____

Purpose:

To provide a HIPAA compliant security policy in regards to ePHI on practice owned and non- organization owned devices.

Definitions:

ePHI: Electronic protected health information.

Bring Your Own Device (BYOD): a non-practice owned device that potentially has access or stores ePHI, typically a mobile device such as a smart phone, tablet, laptop computer, etc.

Complex Password: password containing a minimum of 6 characters using both upper and lower case letters and at least 1 number. Password cannot contain any or all of the user's name, pet's name, or other family member.

Sensitive ePHI: Any patient information that could have a significant impact, financial or reputational, to the patient if the information was disclosed in an unauthorized manner. Example would be results of Serological Testing, before and after photos of patients, etc.

Policy Coverage:

This policy covers the following HIPAA Security Rule Standards:

- § 164.308(a)(3) **Workforce Security:** All ePHI stored on a mobile device must be protected by password access and data encryption;
- § 164.308(a)(6) **Security Incident Procedures:** Users required to report lost or missing devices;
- § 164.310(d)(1) **Device and Media Control:** Device is lost or removed from service, ensure ePHI is removed from device;
- **Mobile Device Usage Agreement.**

To Secure Mobile Devices:

Organization will enable the following supported security policies:

- Remote wipe capability.
- Enforce password on device.
 - Minimum required for non-sensitive ePHI is 4 digit passcode, minimum required for mobile devices storing, receiving or sending sensitive ePHI is a complex password.
 - Using a complex password on an iPhone encrypts all data on the device.



Email Must Be Encrypted At Rest & In-Transit

REQUIRED. PERIOD.

Email from provider to provider.

Emailing within your practice.

Patient sends an email message to doctor.

Why does the hospital send my doctor unencrypted email with PHI?

Beware the “OK” Button

If You Agree To "Oath" You Are Giving Them "**Consent To Access Your Device and Use Your Data**". This May Result In A HIPAA Breach That Could Cost You Millions.

Oath: Excerpts from Terms of Service

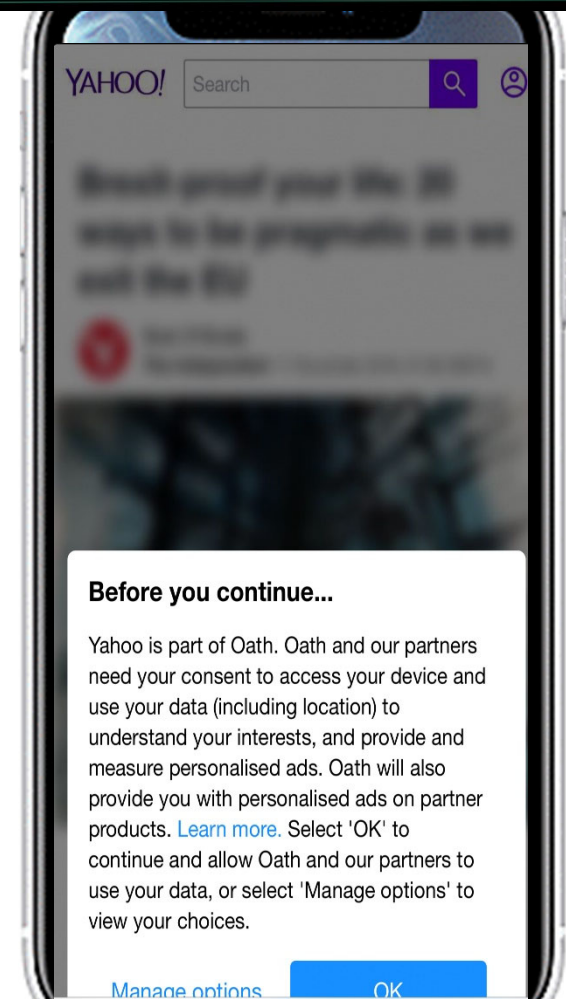
We may collect the information that you provide to us, such as: When you create an account with an Oath Service or brand. (Please note, when you use our Services, we may recognize you or your devices even if you are not signed in to our Services.) When you use our Services to communicate with others or post, upload or store content (such as comments, photos, voice inputs, videos, emails, messaging services and attachments). Oath analyzes and stores all communications content, including email content from incoming and outgoing mail.

When you sign up for paid Services, use Services that require your financial information or complete transactions with us or our business partners, we may collect your payment and billing information.

Device Information. We collect information from your devices (computers, mobile phones, tablets, etc.), ...

Location Information. We collect location information from a variety of sources.

Privacy First: Read Before You Agree.



Build a Culture of Compliance



Monthly System Activity Review Report

Sanctions Given to Workforce Members

Breach Security Risk Assessments

Breach Reporting to OCR

On-Going Staff Training

If's It's Not Documented, It's Not Done.

The Real Cost of HIPAA Violations

**Loss of Trust Between You
and Your Patients**

Loss of Reputation.



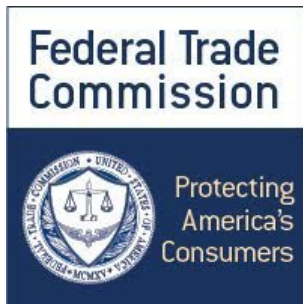
HIPAA IS ALL ABOUT THE DOCUMENTATION YOU CAN SHOW



**“We ask for a lot
of documentation
because the law
requires it.”**



Iliana Peters: Health Information Privacy Specialist
Office for Civil Rights
U.S. Department of Health & Human Services



Federal Trade Commission



**FTC – Unfair Trade Practices Applies
if you are not HIPAA Compliant**

More Joint Investigations With OCR

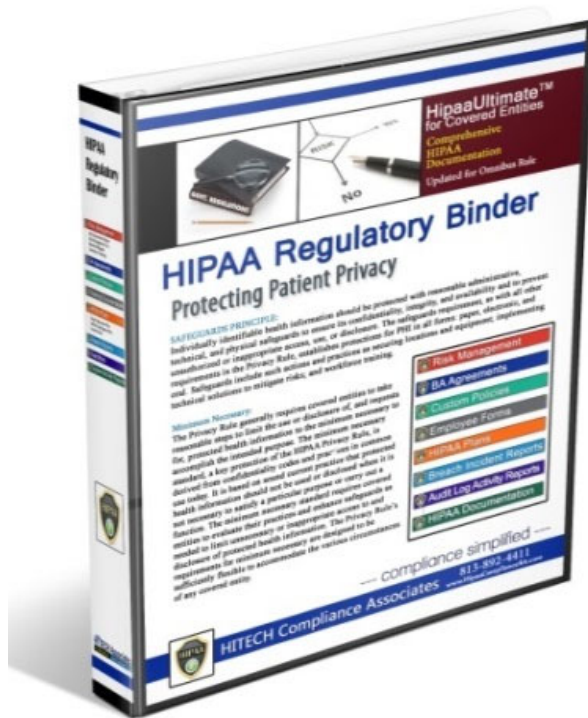
20 Year Oversight of Your Practice



QUESTIONS

COMPLIANCE
REGULATIONS
GUIDELINES

THANK YOU



HIPAA Services






- Risk Assessment
- Policies and Procedures
- Training
- HIPAA Security Officer Certification
- Breach/Ransomware Consulting

www.HipaaComplianceKit.com
mm@HipaaComplianceKit.com

813-892-4411



HIPAA Compliance Kit

 STEP 1	Risk Assessment
 STEP 2	Business Associates
 STEP 3	Policies & Procedures
 STEP 4	HIPAA Training
 STEP 5	Breach Plan
 STEP 6	Contingency Plan
 STEP 7	Documentation
 STEP 8	System Activity Review