# HIPAA Awareness Training 2017

# HIPAA is Federal Law

HIPAA is enforced by HHS Office for Civil Rights

A Part of Health & Human Services

HIPAA Can Also Be Enforced By
State Attorney Generals

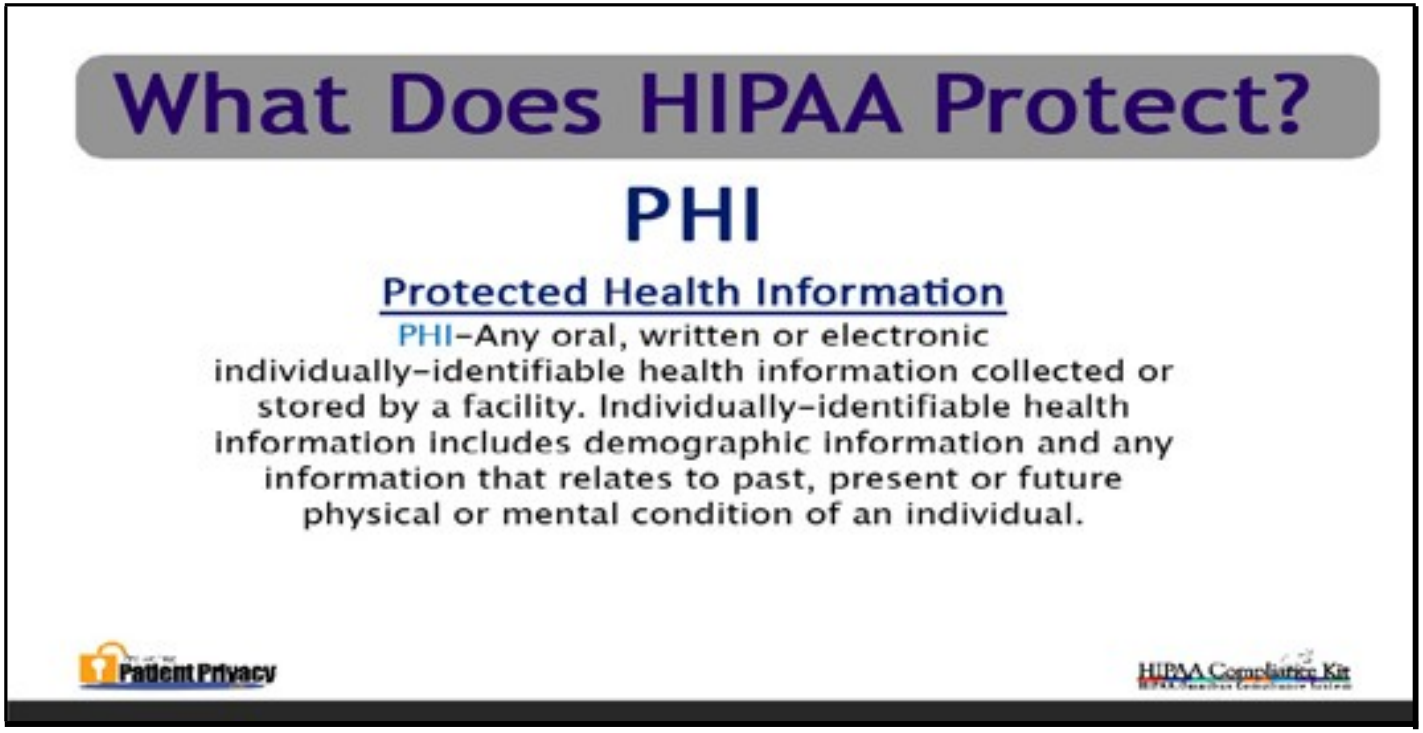
Office for
Civil Rights

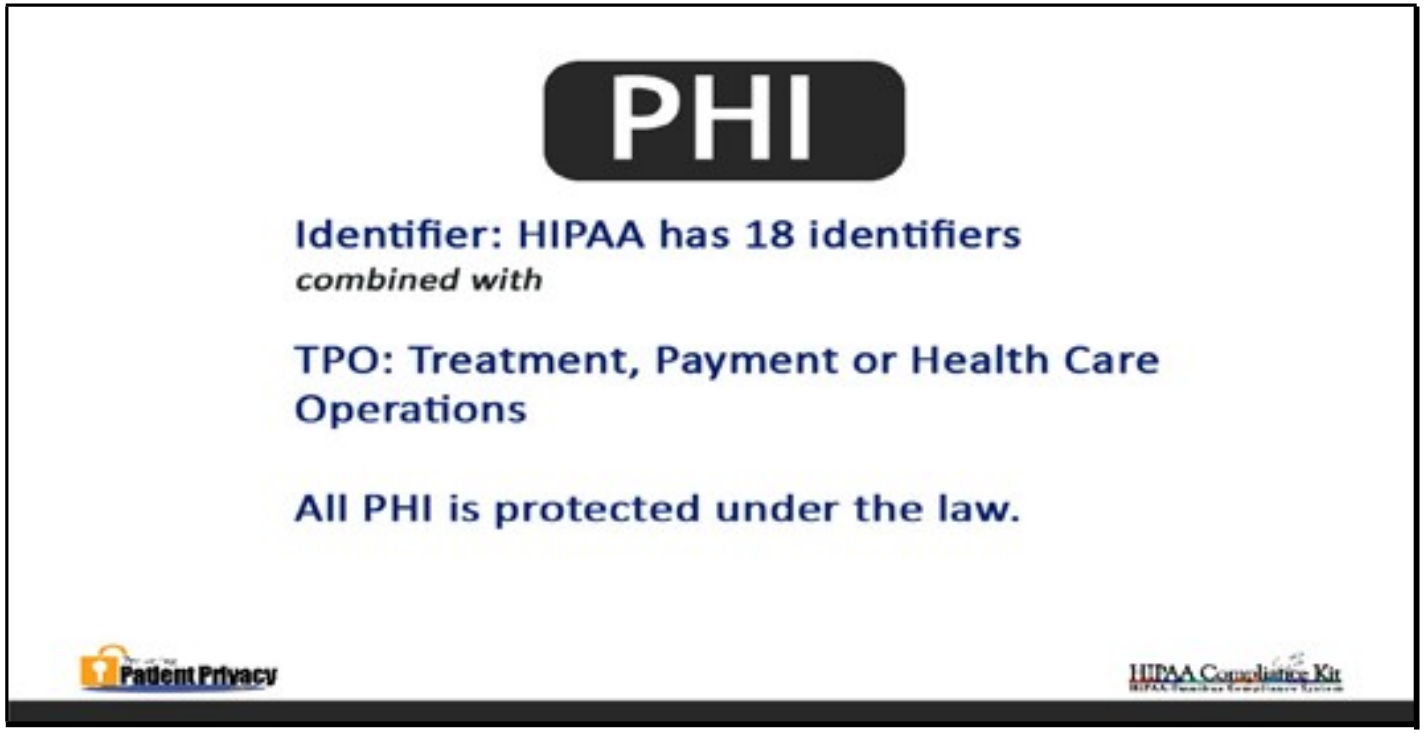
Patient Privacy

HIPAA Compliance Kit

# Protecting Patient Privacy

- Think of HIPAA as a basic set of guidelines to help your practice protect patient privacy.


What Does HIPAA Protect?
PHI
Protected Health Information
PHI-Any oral, written or electronic individually-identifiable health information collected or stored by a facility. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.
Patient Privacy
HIPAA Compliance Kit


PHI
Identifier: HIPAA has 18 identifiers
combined with
TPO: Treatment, Payment or Health Care Operations
All PHI is protected under the law.
Patient Privacy
HIPAA Compliance Kit


sPHI can include:

- Psychotherapy notes (which are not a part of the official medical record)
- Information about genetic testing
- Information about HIV/AIDS testing or treatment
- Domestic Abuse/Violence
- Information about child abuse or neglect
- Information about sexual assault

# Minimum Necessary

A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. **A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.** A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.


# This Training Will Focus On:


Patient Privacy Rights

Breach Notification Requirements

HIPAA Security Rule

Patient Privacy

# Patient Privacy Rights

Right to Inspect or Get Copies of their Designated Record Set

Right to Request Amendment of the Medical Records

Right to Request Confidential Communications

Right to Request An Accounting of Disclosures

Right to Request Restrictions on The Sharing of Their PHI

Right to Restrict Information from Their Health Plan for Services Paid in Full

Right to Receive Your Notice of Privacy Practices

Right to File A Privacy/Security Complaint

Patient Privacy

HIPAA Compliance Kit

# Right to Access

A patient may make a request to access or receive a copy of his or her medical record as it is kept in the designated record set. Omnibus updated this right to include all records maintained by the practice or their business associate.

For your office to require the request to be in writing on your form the patient must be informed of this policy prior to their request.

# Right to Access

The Privacy Rule requires a covered entity to provide the individual with access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed to by the covered entity and individual. **If the individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format**, if it is readily producible in that form and format, or if not, in an agreed upon alternative, readable electronic format.

# Right to Access

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:

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.

To use a web portal for requesting access, as not all individuals will have ready access to the portal.

To mail an access request, as this would unreasonably delay the covered entity's receipt of the request and thus, the individual's access.

# Verification

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access.

Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access - whether in person, by phone (if permitted by the covered entity), by faxing or e-mailing the request on the covered entity's supplied form, by secure web portal, or by other means.

You must document that you verified the identity of the patient.

# Right to Access

**Where an individual requests an electronic copy of PHI that a covered entity maintains only on paper, the covered entity is required to provide the individual with an electronic copy if it is readily producible electronically (e.g., the covered entity can readily scan the paper record into an electronic format) and in the electronic format requested if readily producible in that format.**

Where an individual requests an electronic copy of PHI that a covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format. A covered entity may permit an individual to do so, and covered entities are encouraged to offer individuals multiple options for requesting access.

# Right to Access

A covered entity also must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pick up a copy of the PHI or to inspect the PHI (if that is the manner of access requested by the individual), or to **have a copy of the PHI mailed or e-mailed**, or otherwise transferred or transmitted to the individual to the extent the copy would be readily producible in such a manner.

Mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI while in transit (such as where an individual has requested to receive her PHI by, and **accepted the risks** associated with, unencrypted e-mail). Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed.

# Right to Access

## Individual's Right to Direct the PHI to Another Person

An individual also has a right to direct the covered entity to transmit the PHI about the individual directly to another person or entity designated by the individual.

# Right to Access

The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible. Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI requested through personal health records, web portals, or similar electronic means.

Further, individuals may reasonably expect a covered entity to be able to respond in a much faster time-frame when the covered entity is using health information technology in its day to day operations.

# Right to Access

## Fees for Medical Records Per OCR Guidance

3 Methods for Charging Allowed

1) Actual Costs
2) Flat Fee - $6.50 and must include postage.
3) Average Costs

Documentation Must Be Kept on Average Costs and Method to Determine Actual Cost.

# Right to Access

## Reviewable grounds for denial (45 CFR 164.524(a)(3)).

A licensed health care professional has determined in the exercise of professional judgment that:

1. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
2. The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
3. The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

# Request to Amend

The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set **when that information is inaccurate or incomplete**. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a **written denial** and **allow the individual to submit a statement of disagreement for inclusion in the record**. The Rule specifies processes for requesting and responding to a request for amendment. ***A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.***

# Request for Confidential Communications

Covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.

For example, an individual may request that the provider communicate with the individual through a designated address or phone number.

# Request to Disclose Accounting

Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request.

# Request to Disclose Accounting

The Privacy Rule does **not require accounting for disclosures:**
(a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

# Request to Disclose Accounting

Examples of Disclosures Your Office Must Track.

**EXAMPLES**

State mandated reporting (such as suspected abuse or neglect victims, disease reporting such as STDs, brain injuries, dog bites, etc.)
Cadaveric organ, eye, or tissue donation purposes.
Disclosures required by law (Gun shot wounds, victims of a crime, reporting a crime in emergencies, court order or court-ordered warrant).
Decedents: Funeral Home Directors, Coroners and medical examiners.
Faxing patient information to the wrong location or to the wrong clinician (All Breaches)
Disclosure of patient information outside of a "need to know"

**Standard accountings must include:**

1. Date of disclosure;
2. Name of the recipient, and address if known;
3. Brief description of the PHI disclosed;
4. Brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for disclosure, or a copy of the request for the disclosure.

# Request To Restrict Use or Disclosure of PHI

Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

**What is in the patient's best interest?**

# Requirement To Restrict Use or Disclosure of PHI

A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if the disclosure is for the purposes of carrying out payment or health care operations and not otherwise required by law; and the protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full."

# Notice of Privacy Practices

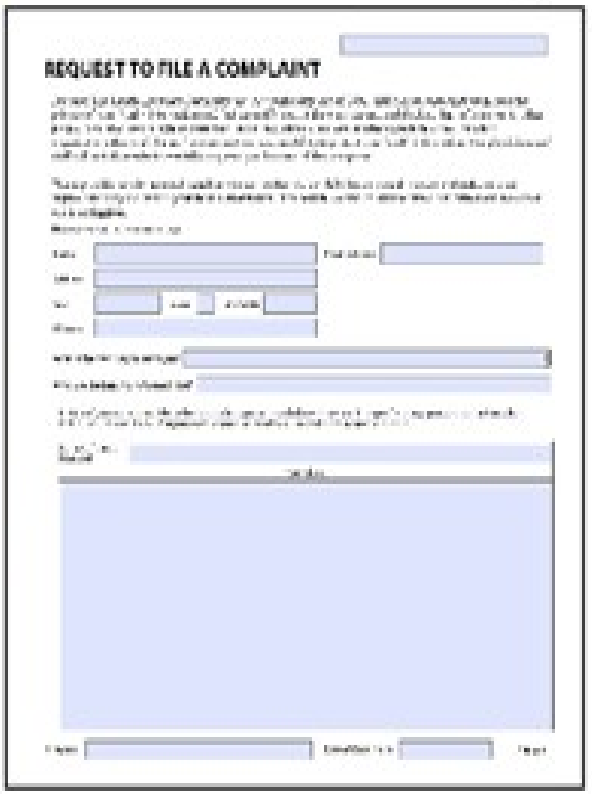
**Covered entities must act in accordance with their notices.**

Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. **The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated.**

# Notice of Privacy Practices

## Patient Privacy (HIPAA) Complaint Form

Give Your Patients A Process To File A Privacy Complaint or they will use the forms the Office for Civil Rights provides on their web site.

# Notice of Privacy Practices

## Notice Distribution.

Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);

By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and

In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Receipt of Notice of Privacy Practices Must Be Signed Every 3 Years.

# Uses & Disclosures

**Only 3 Types of Disclosures Are Permitted Under the HIPAA Laws**

**Required** – Government (HHS, OCR, CMS, OIG)
Government does not include law enforcement.

**Authorized** – Patient Not Subject to Minimum Necessary.

**Permitted:**
Uses and disclosures between covered entities.
Uses and disclosures to a Business Associate.
Uses and disclosures pursuant to a valid HIPAA authorization.
To the patient.

# Authorization Form

## Elements

Description of PHI to be used or disclosed (identifying the information in a specific and meaningful manner).

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

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

Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.

Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).

Signature of the individual and date. If the Authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual.

## Authorization Required Statements

The individual's right to revoke his/her Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.

Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.

The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.

# Subpoena Requests


With Authorization – Ensure Authorization has all 9 (nine) required elements.

Notice of Production – Some states allow for medical records to be released if the Subpoena includes a "Notice of Production".

Court Order – Signed by a Judge, follow all instructions on the Order.

# Omnibus Breach


*A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.*

# Omnibus Breach

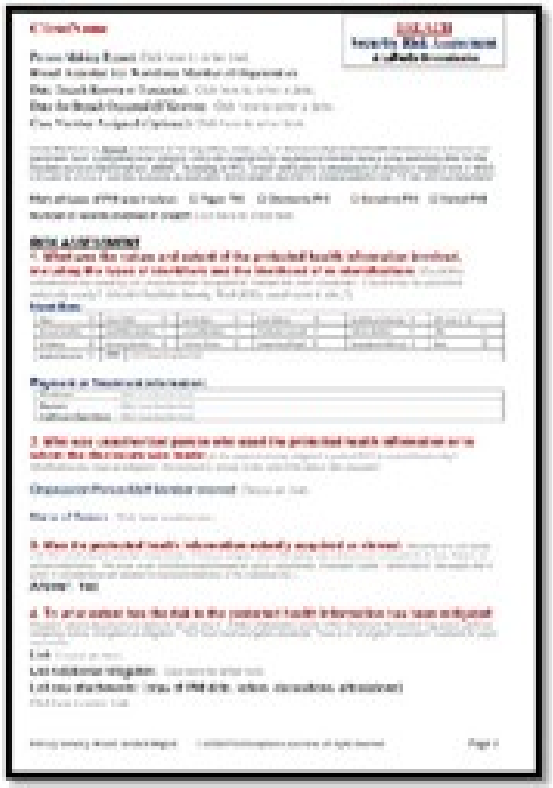
1. Misdirected faxes containing PHI
2. PHI provided to the wrong requestor
3. PHI given without authorization
4. Inappropriate disclosure to employer
5. Identity theft
6. Stealing and disclosing PHI
7. Sensitive information lost (media or paper)
8. Inappropriate access – Violates Minimum Necessary
9. Confidential Communication Violations

# Breach Risk Assessment

A Breach Security Risk Assessment must be performed for every suspected breach to determine if a breach occured.

**4 Questions Are Critical To This Process**

1. What was the PHI that was involved
2. Who was the person(s) that accessed the records
3. Was the PHI viewed or acquired
4. How have you mitigated the risk to the PHI



Patient Privacy

# Breach Response

Our practice has legal requirements in the event of a breach of PHI.

The HIPAA Privacy Officer must immediately be notified of any suspected breach.

Following your practice's policies and procedures will greatly reduce the occurance of breaches.

Patient Privacy

HIPAA Compliance Kit

# HIPAA Security Rule

The Security Rule dictates the Policies and Procedures, Security Measures, and other methods used to protect ePHI.

Examples: Unique User IDs, Complex Passwords, Automatic Logoff After Period of Inactivity, and Yearly HIPAA Training.

Patient Privacy

HIPAA Compliance Kit

# HIPAA Security Rule

Medical Records are a Prime Target for Cybercriminals

- Medical Identity Theft
- IRS Refund Fraud
- Medicare Fraud
- Credit Card Fraud
- Other Financial Fraud

Patient Privacy

HIPAA Compliance Kit

# Security Risks

Reduced by a "Culture of Compliance"
or following your policies and procedures.

- Security is 25% Computer Countermeasures,
- 75% Employee Behavior.

# Security Risks

## Cybersecurity Awareness

Think twice before clicking.

Never disable security controls such as anti-virus, firewalls or otherprotective measures that IT has put into place.

Do not install screen savers or other programs without prior approval.

Unless allowed for specific reasons, cell phones should not be on the desk and never charge your cell phone using your computer's USB connection.

# Physical Security

## The Security Rule Requires Physical Protections of PHI

Charts, forms faxes and other information containing patient information should be placed faced down.

When you leave your workstation, press Control L.

**Do not throw away paper with PHI. (Post-It Notes)**

Clear your work area of PHI before leaving for a break.

**Never leave your web browser open when it is not in use.**

Lock your area if possible.

**Turn it over, turn it on.**

HIPAA Compliance Kit

# Critical Security Protections

## Protecting the Privacy of Patient Medical Records

1. Complex Passwords, Changed Every 90 Days
2. Email Awareness and Security
3. Understanding Web Browsing Dangers

HIPAA Compliance Kit

# Critical Security Protections

## Complex Passwords, Changed Every 90 Days

MicHa?lMcco45Y

**2 Rules**

Capitalize every 4th letter.
Replace every e with a ?.

**Check password strength Microsoft Secure Web Site:**
https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Banner_Password_Checker

# Critical Security Protections

**Brute Force Attacks Can Try Thousands of Combinations Per Second.**

Top 10,000 Passwords are used by 98.8 % of all users.

4.7% of users have the password password;
91% have a password from the top 1000 passwords

**Most Common Passwords Used in 2015**

| | | |
|---|---|---|
| PASSWORD | DRAGON | MASTER |
| 123456 | MONKEY | LETMEIN |
| QWERTY | PRINCESS | STARWARS |
| FOOTBALL | BASEBALL | 12345678 |

(as determined by SplashData)

Patient Privacy

HIPAA Compliance Kit

# Critical Security Protections

## Do Not Cross Your Passwords

Use separate passwords for work and home.

# Critical Security Protections

## Email Awareness & Security

www.localhospitall.com

Always verify the email address, to the letter.

Do not open attachments
Unless you expect the email with the attachment
Have verified the attachement was sent by a trusted source

# Critical Security Protections

Think Twice Before You Click.


Think Twice Before You Click.

Patient Privacy

HIPAA Compliance Kit

Bitcoin is internet “money” that hackers will charge you in order to get your data back after they have stolen it.

# Critical Security Protections

## Understanding Web Browsing Dangers


Just visiting an infected web site can download malicious software on to your practice's network.

Only use the web for work related purposes, even on your own time to protect patient privacy.

Do not connect your personal device (cell phone) to the practice's wireless network or with a USB cable.

Patient Privacy

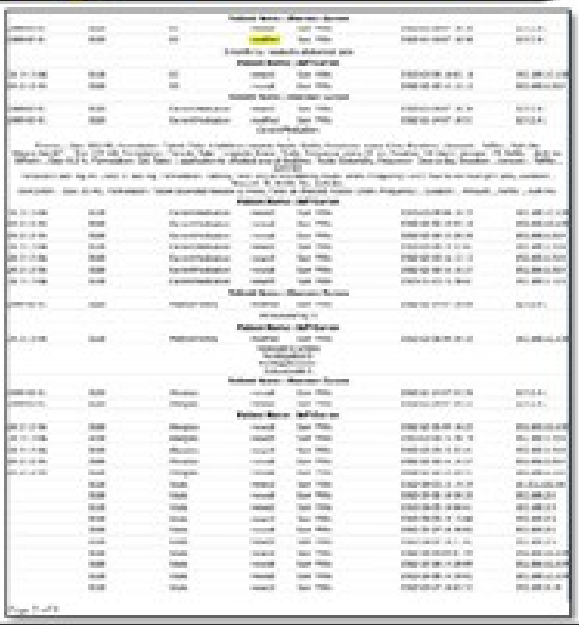
HIPAA Compliance Kit

# HIPAA Security Rule

EMR's Produce Audit Log Activity of All User Access to Patient Records

Your HIPAA Compliance Office must review and report on these logs

You may be asked about any unusual or suspicious activity that is recorded on your unique user ID



Patient Privacy

# Cell Phone Dangers

- Camera for improperly Recording PHI
- Easily Lost, Stolen or Discarded with PHI
- Access to EHR
- Access to email and text messaging with PHI
- Easy Access to Facebook for improperly Posting PHI
- Microphone and Camera Accessed and Turned On
- USB Connections Permit Unauthorized File Transfer

Patient Privacy

HIPAA Compliance Kit

# RansomWare

## 4000 Ransomware Attacks Per Day

Up from 1000 Attacks Per Day in 2015

58% of Victims Unable to Recover Data

93% of Phishing Emails Are Delivering Ransomware


Patient Privacy

HIPAA Compliance Kit

# RansomWare

## Healthcare is the Number 1 Target for Ransomware

Healthcare is 4.5 times more likely that other companies and industries to be attacked.


Patient Privacy

HIPAA Compliance Kit

# RansomWare

## PRECAUTIONS

Never disable your anti-virus or anti-malware.

Do not click on an update link for any software including Adobe Reader, Java, Windows, etc.

Do not click on a link to upgrade security software or respond to a request to run a anti-virus scan.

Never surf the internet at work or use the internet for non-work purposes.

Never check your personal email from your office computers.

When in doubt, do not click on a link or download an attachment.

Think twice before you click.

# RansomWare

## EMAIL PRECAUTIONS

Double check the return email address of the sender.

Check the return address to the letter. films@raddiologycenter.com

Do not click on a link or download an attachment unless you were expecting the file or have called to verify that the attachment is from a known source.

After you download a file, review the download folder and verify that the downloaded file has the correct extention, ie, .pdf, .docx. Immediately delete the file if it has .exe or .bat

# RansomWare

## Social Engineering - Attacking the Human Element

Cybercriminals use fear, urgency, curiosity and sympathy to trick you into clicking their link.
And remember, there is no such thing as a free lunch, criminals love to use the word "FREE".

**Other Social Engineering Attacks**

**Clickbait** - look at this.

**Watering Hole Attacks** - Cybercriminals infect sites they know you like to visit.

**Social Networking** - the cybercriminal uses known information about you to trick you into clicking.
Lock down your privacy settings on social media so criminals cannot use your information to trick you.

**US Department of Justice/FBI Cybercrime Division** - you can avoid legal troubles by paying a fine.

Phishing/Spear Phishing - looks like it is coming from a legitimate source; bank, hospital

# RansomWare

## Social Engineering


Use Common Sense

Trust your gut feeling.

If it feels to good to be true, it probably is.

Feels slightly off, probably is.

Stop and think about what is being asked of you.

How did they get my phone number, email address, etc...

# RansomWare

## Signs Your Network Has Been Infected

*Report Any Suspicions Immediately*

1. You can't find files;
2. Your computer has noticibly slowed down;
3. Realization that a link or file attachment opened or a website visited may have been malicious in nature.

# RansomWare

## Infected or Suspect Your Computer Has Been Infected

- Power off your computer;
- Disconnect the network cable from the computer;
- Notify your supervisor immediately;
- Alert other staff members;
- Change all passwords;
- Contact Law Enforcement - FBI and/or Secret Service.

FBI: fbi.gov/contact-us/field
Internet Crime: ic3.gov/gov/default.aspx

Patient Privacy

HIPAA Compliance Kit

# Incidental Use & Disclosure

The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated.
A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has ***adopted reasonable safeguards*** as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.

See Reasonable Safeguards in HIPAA Essentials Training Manual

# Incidental Use & Disclosure - sPHI

Sensitive Protected Health Information requires additional steps to help safeguard information that could harm the patient financially, reputationally or emotionally.

1. Make sure you are behind a closed door when discussing sPHI.
2. Speak in the lowest volume to communicate the information to the patient.

# Protecting Patient Privacy

## Everyone's Responsibility

1. Protect the Patient From the Harm A Breach Could Cause.
2. Maintain the Reputation of Your Practice.

Patient Privacy

# Medicare Fraud

Medicare fraud is typically characterized by:

Knowingly submitting false statements or making misrepresentations of fact to obtain a federal health care payment for which no entitlement would otherwise exist;

Knowingly soliciting, paying, and/or accepting remuneration to induce or reward referrals for items or services reimbursed by Federal health care programs; or

Making prohibited referrals for certain designated health services.

# Medicare Abuse

Abuse describes practices that, either directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse includes any practice that is not consistent with the goals of providing patients with services that are **medically necessary**, meet professionally recognized standards, and priced fairly.

# Medicare Fraud & Abuse

Federal laws governing Medicare fraud and abuse include the:

- False Claims Act (FCA);
- Anti-Kickback Statute (AKS);
- Physician Self-Referral Law (Stark Law);
- Social Security Act; and
- United States Criminal Code.

# Medicare Fraud & Abuse

## Be Part of the Solution, Not Part of the Problem.

Report suspected Fraud and Abuse.
OIG Hotline: Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950;

Fax: 1-800-223-8164; Email: HHSTips@oig.hhs.gov

Online: https://forms.oig.hhs.gov/hotlineoperations

Mail: U.S. Department of Health & Human Services

Office of Inspector General
Attn: OIG Hotline Operations
P.O. Box 23489
Washington, DC 20026

# OCR Documentation Audits

The Office for Civil Rights has announced documentation audits

Your Practice must show ongoing HIPAA compliance through documentation

Sanctions show that your practice has a "Culture of Compliance"


Patient Privacy

HIPAA Compliance Kit

# Documentation

## If it is not documented, it's not done.

Use HIPAA Kit forms to document requests for access, disclosure and patient privacy concerns.

Patient Privacy

HIPAA Compliance Kit

# Security is a Balance

## Good Health Care vs. Privacy

**HIPAA and the Omnibus Updates to HIPAA has the goal to improve healthcare.**
You should always error towards good health care.
Many times you will need to make a judgment call on providing quality health care or protecting the privacy of an individual. Always seek the advice of the HIPAA Privacy Officer, Physician or Office Manager. There will be circumstances where they are not available in the time frame needed so use your best judgment, common sense and error towards providintg quality health care.

Patient Privacy

HIPAA Compliance Kit