HIPAA Update 2018

Presented by
Michael Brody, DPM

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Objectives:

- Understand Patient Rights under HIPAA
- Learn practices to minimize the possibility of a HIPAA Breach
- Understand that HIPAA compliance is more than just keeping data secure

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Introduction

- In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). Revisions have been made public and the full implementation of the rule became effective April 14, 2003.

In Addition to HIPAA

- There may be local and state privacy regulations that you are required to follow
- This presentation does **NOT** cover any local regulations

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Viewing Patient Records

- You may not access a patients record unless it is in performance of your job for care of the patient or for billing purposes
- You must have an authorization or other legal authority (e.g., waiver of HIPAA authorization for research) in order to access for any other reason
- Browsing a patients health record for personal reasons or out of curiosity is strictly prohibited
  - Appropriate disciplinary action may be taken

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Healthcare

Who	43% external, 56% internal
What	79% medical, 37% personal, 4% payment
How	35% error, 24% misuse

Healthcare is the only industry where the threat from inside is greater than that from outside. Human error is a major contributor to those stats. Employees are also abusing their access to systems or data, although in 13% of cases, it's driven by fun or curiosity – for example, where a celebrity has recently been a patient.

Source: Verizon Business 2018 Data Breach Investigations Report.

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Protected Health Information (PHI)

- Protected Health Information is all Personally Identifiable Information that is held or transmitted
- This includes:
  - Written information
  - Information stored in computer systems
  - Information transmitted orally

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Personally Identifiable Information

- Personally Identifiable Information (PII) refers to any information about an individual including:
  - any information which can be used to distinguish or trace an individual's identity and
  - any other information that is linked or linkable to an individual

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Examples of PII

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above examples

When can information be disclosed?

- When the patient has provided written permission
- Legal Authority permits disclosure without written authorization
- When the information is being provided to another provider who is treating the patient (Covered Entity)
- When the information is being provided to a Business Associate and there is a valid Business Associate Agreement in place

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Covered Entity vs Business Associate

- A Covered Entity has a DIRECT relationship with the patient
  - If the organization bills the patient for services they are a covered entity
  - If the organization bills YOU for services they are a business associate

After you complete a permitted disclosure

- The information is NOW out of your control
- This is why a disclosure log is EXTREMELY important
- If information is breached after you complete a permitted disclosure
  - IT IS NOT YOUR RESPONSIBILITY

PICA
Treated Fairly
Underwritten by a ProAssurance Company

PII and Marketing

- PII can not be used for external marketing purposes without the explicit permission of the patient

- PII can be used for internal marketing purposes. A doctor can market services to his/her patients based upon information in their medical record.

PICA
Treated Fairly
Underwritten by a ProAssurance Company

PII and Public Health

- PII can be disclosed to Public Health Agencies for population health activities. This can include but is not limited to:
  - Bio Surveillance
  - Immunization Registries
  - Cancer Registries
- Any other disclosure that is important to public health and safety

PICA
Treated Fairly
Underwritten by a ProAssurance Company

There are many causes of privacy breaches:

- Carelessness
- Ignorance
- Information system vulnerabilities
- Flawed policies and procedures
- Criminal behavior

PICA
Treated Fairly
Underwritten by a ProAssurance Company

What about Security Breaches?

- We are custodians of our patients medical records and we need to be responsible custodians
- To do your part in protecting the information, you must protect:
  - your equipment,
  - any documents and to which you have access, and
  - any sensitive information with which you might be working
- You should ensure that equipment and information are kept in a secure place
- Each practice must have a Security Officer
  - If an incident occurs, report it to your Security Officer immediately

PICA
Treated Fairly
Underwritten by a ProAssurance Company

The Three Pillars of HIPAA

- Confidentiality
- Integrity
- Availability

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Confidentiality

- Confidentiality means that personal, sensitive, or protected information is available only to those people who need it to do their jobs

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Your Role in Confidentiality

- Understand what information you have access to and why
- Take appropriate steps to protect PII, network access, passwords, and equipment
- Don’t use automatic password-saving features found on websites
- If sensitive information has been compromised, report the incident to your Security Officer
- Failure to report incidents is a HIPAA violation

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Integrity

- Integrity means that the patient's chart is correct

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Your Role in Integrity

- Should you make a mistake in a chart such as charting the wrong information or putting information from one patient into another patients chart, make sure this is corrected
- When making corrections always be aware of the Medical-Legal implications of changing information in patient charts and do it in a proper manner

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Availability

- Means that a patients information is available to you and your practice when it is needed for care of that patient
- What good are medical records if they can not be read when they are needed?

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Your Role in Availability

- Do not use practice computers in a manner that may cause ‘traffic jams’ on the computer network
- This includes activities such as:
  - Streaming Media
  - Downloading Files
  - Sharing photos and music

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Privacy and Security Officers

- Every practice MUST appoint a Privacy and Security Officer
- One person can have both roles
- Know who the Privacy and Security Officers are at your practice

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Privacy and Security Officers can help with:

- Knowing what to do if PII has been wrongfully disclosed
- Knowing what to do if your computer is infected with a virus
- Knowing what to do if you find or suspect someone using computers inappropriately or using them for theft or fraud
- Understanding your role in protecting the privacy, confidentiality, and integrity of sensitive information

PICA
Treated Fairly
Underwritten by a ProAssurance Company

HIPAA Enhanced

- With HITECH – the law that gave us the incentive to implement EHR technology, there were additional rules added to HIPAA this is known as HIPAA Enhanced
- HITECH also increases the potential legal liability for non-compliance and it provides for more enforcement

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Enhancements include:

- Establishing a notification system in case unauthorized disclosure takes place
- Expanding privacy rules to entities that do work on behalf of providers and insurers
- Providing audit trails of all electronic record disclosure
- And increasing penalties for violations

PICA
Treated Fairly
Underwritten by a ProAssurance Company

When is Criminal

- When a HIPAA violation is deliberate it is a criminal offense, especially if malice or intent to harm can be demonstrated

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Civil Penalties Apply

- When the HIPAA violation was not caused intentionally

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Disclosure Rules of Thumb

- When disclosing PII only disclose the minimum amount of information necessary
- When possible all data that can should be de-identified
- Any data that is not necessary should not be disclosed.
  - Disclosure of un-necessary data even in an authorized manner can be considered a HIPAA violation.

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Up Until 2013

- The only entities that received HIPAA fines had breaches of 500 or more patients
- In January 2013, ONC (The HIPAA Police) fined an organization for a breach that impacted less than 500 patients
- Enforcement of the HIPAA Regulations is increasing
- Audits for HIPAA compliance have started

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Patient Rights

- Under HIPAA patients have the right to:
  - Receive a notification from every provider about their privacy rights and the providers privacy policies
  - Request copies of their Medical Records
  - Receive an accounting of all disclosures of their PII
  - Request changes to their Medical Records
- Providers are required to comply with the first three items

PICA
Treated Fairly
Underwritten by a ProAssurance Company

And…

- Patients have the right to file complaints regarding your practices HIPAA practices

- Your practice PRIVACY OFFICER is the person who the patient must have access to when they have questions about your practice HIPAA practices

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Patients E-Rights

- Patients can place restrictions on how their electronic records are shared for purposes related to treatment
- Providers are NOT required to comply with these requests, but must document and respond to the request

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Patients E-Rights

- Patients can place restrictions on how their electronic records are shared for payment purposes if they have paid for their care and an insurance company or third party is not involved in payment

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Patients E- Rights

- Patients have a right to an electronic copy of their medical record
- Providers can charge a reasonable fee for supplies, labor, and postage for this service

PICA
Treated Fairly
Underwritten by a ProAssurance Company

HIPAA Details

- Patients rights under HIPAA survive even after the patient has expired
- The personal representative of a deceased individual (e.g. Executor of the Estate) has the same rights as the deceased individual
- Parents have rights to PII of their dependent children
- Legal guardians do not have rights to PII unless specifically enumerated

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Disposal of Records

- Records may not be disposed of without proper disposition authority
- Follow your local policies and procedures for disposing of printed paper copies containing sensitive information by contacting your Security Officer for media destruction procedures
- These documents should be destroyed to a degree that renders them incapable of being read or reconstructed

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Disposing of Computers

- Privacy issues arise when it is time to retire old computer equipment
- Here is what you can do to prevent such issues from arising:
  - Ensure that sensitive information stored on computers is disposed of properly before it is removed from service
  - If you see computers being thrown out without proper disposal, let your Security Officer know
  - Understand the concept that clicking the Delete button doesn't really delete a file completely from your computer

Importance of Passwords

- Passwords are important tools for protecting information and information systems and getting your job done
- They ensure that you and only you have access to the information you need
- Keep your password secret
- If you have several passwords, store them in a safe and secure place that no one else knows about

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Email Privacy and Security

- Don’t expect privacy when using email to transmit, store, and communicate information
- Email is a great tool on which we have come to depend to do our jobs faster, but using email also has risks
- Use it appropriately to protect information, and take certain precautions to reduce the risk of spreading viruses

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Fax Security

- Users should transmit sensitive information via fax only when there is no other way to provide the requested information in a reasonable manner or timeframe
- If you must fax sensitive information, the following security controls must be implemented:
  - Use a disclaimer fax statement on all cover sheets
  - Double-check the recipient's fax number prior to sending the fax
  - Contact the recipient prior to sending the fax to ensure that he or she is available to retrieve it and to ensure that the fax machine is located in a controlled area
  - Ask the recipient to confirm receipt of the fax
  - Save transmittal summaries for periodic review
  - Remind regular fax recipients to provide notification if their numbers change

Laptop Security

- Protection of data stored on laptops is a very important component in securing our patients' data
- Laptops can contain large amounts of data that could fall into the wrong hands if proper precautions are not taken

Removable Storage Media

- Any media—thumb drives, external ports, etc.—that connect to practice resources should be encrypted
- These are small and easily lost or misplaced so extra precautions need to be taken to protect removable storage media

Social Engineering Methods

- A social engineer may try to trick you into revealing your password to gain access illegally to your system or to information about patients and employees
  - We know you want to be helpful, but social engineers may try to take advantage of your kindness
- If people ask you for Sensitive Personal Information, make sure you know who they are and whether they have proper authority for access to the information

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Malware

- High-tech vandals have created dangerous programs that infect computer systems
- These programs vary in how they infect and damage systems, and are collectively called malware
- When our systems become infected with malware, they may not operate properly
  - Viruses
  - Worms
  - Trojan Horses
  - Malicious Emails

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Malware Symptoms

There may be a problem if your computer has any of these symptoms:

- Reacts more slowly than usual
- Stops running for no apparent reason
- Fails to start (“boot”)
- Seems to be missing important files
- Prevents you from saving your work

PICA
Treated Fairly
Underwritten by a ProAssurance Company

What are Information Security Incidents

Security incidents include the following:

- Lost or stolen portable equipment—causes major security breaches. These data breaches violate our promise to our patients and put them at risk for identify theft.
- Virus attack
- Faxing PII
- Missing or compromised files
- Improper disposal of PII
- Mailing PII—Make sure you mail information to the proper person
- Unattended personal information
- Accessing or sharing Sensitive Personal Information (SPI) with people who do not have a need to know
- Sending unencrypted emails containing PII

PICA
Treated Fairly
Underwritten by a ProAssurance Company

If you think there has been an incident

If you think a security incident has occurred, you should…

- Write down:
  - The date, time, and location the incident took place, as well as the computers which may have been affected
  - Any error messages that showed up on your computer screen
  - Any web addresses, server names, or IP addresses involved in the incident

PICA
Treated Fairly
Underwritten by a ProAssurance Company

If you think there has been an incident

- Contact your Privacy and Security Officer in person or by telephone rather than by email
- If a crime is involved, report it to law enforcement
- Protect yourself – if you witness what you believe to be a security or privacy incident, you are obligated to report it
- If you fail to report such an action, you may be considered an accomplice to that action

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Preventing Incidents

While at work, always do the following:

- Follow all privacy policies and procedures
- Properly dispose of any private data you no longer need
- Report suspected or potential breaches of privacy to your Privacy Officer or Security Officer
- If you are in doubt, ask your immediate supervisor
- Work as a team to ensure privacy

PICA
Treated Fairly
Underwritten by a ProAssurance Company

You are the first line of defense

- As we learn more about the tactics hackers use to get access to information and computer systems
  - Hackers continue to look for new ways to get around our protections
- Technology is changing at a fast pace and we need to keep up to date with the changing landscape and secure our information systems
- You have to be diligent in protecting the practice, because you are the first line of defense

PICA
Treated Fairly
Underwritten by a ProAssurance Company

Questions??

PICA
Treated Fairly
Underwritten by a ProAssurance Company