



HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA IS ENFORCED BY
THE HEALTH AND HUMAN
SERVICES OFFICE FOR
CIVIL RIGHTS



WHAT DOES HIPAA PROTECT?



PHI = Protected Health Information

PHI – Is 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.

sPHI- Sensitive Protected Health Information. PHI that if breached, could cause the patient financial, reputational or emotional harm.

ePHI- Electronic Protected Health Information that is produced, saved, transferred or received in an electronic form.

PROTECTED HEALTH INFORMATION (PHI)

IDENTIFIABLE PATIENT INFORMATION

Unique Identifiers Including:

- Name
- Address
- Dates of Birth – Dates of Death
- Telephone and Fax numbers
- Email address
- Social Security Number
- Photographic images
- Medical history and treatment
- Health plan beneficiary information
- Financial Information (insurance, credit/debit card numbers)



sPHI - Examples

- Psychotherapy Notes (not part of medical record)
- Information about a Mental Illness or Developmental Disability
- Information about HIV/AIDS Testing or Treatment
- Information about STDs
- Information about Substance Abuse
- Information about Genetic Testing
- Information about Child Abuse and Neglect
- Information about Abuse of an Adult with a Disability
- Domestic Abuse/Violence
- Information about Sexual Assault
- Information about Artificial Insemination



PROTECTING PATIENT PRIVACY

CONFIDENTIALITY, PRIVACY AND INFORMATION SECURITY

Objectives:

- Identify types of confidential information.
- Describe best practices for safeguarding information in spoken, written or electronic formats.
- Understand your responsibility for data encryption.
- Describe your responsibilities for protecting information and reporting violations.
- Identify consequences for violations
- Locate your affiliate's Privacy, Information Security and/or Compliance Offices.

PROTECTING CONFIDENTIAL INFORMATION:

- Access Information *only* if needed to do your job.
- Share information *only* with others who need it to do their jobs.

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 phi needed to accomplish the intended purpose of the use, disclosure or request.



THREE AREAS OF HIPAA TRAINING FOCUS:



PATIENT PRIVACY RIGHTS



BREACH NOTIFICATION REQUIREMENTS



HIPAA SECURITY RULES

Confidential information is stored and shared in the following ways:

- Verbal Communication (talking)
- Paper Documents
- Electronic Data

PATIENT PRIVACY RIGHTS

- Right to inspect or get copies of their records
- Right to request amendment of 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 ACCESS

A patient may place 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



The patient must be informed of any policy to request records in writing PRIOR to their request.

RIGHT TO ACCESS

A covered entity must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pickup a copy of the PHI or to inspect the PHI or to have a copy of the PHI mailed, 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 limited cases 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 associate 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 their PHI if the individual requests that the copy be mailed or e-mailed.

REQUEST TO DISCLOSE ACCOUNTING

EXAMPLES OF DISCLOSURES WHICH MUST BE TRACKED:

- State Mandated Reporting (suspected abuse or neglect, disease reporting such as STD's, 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)
- Faxing patient information to the wrong location or the wrong clinician
- Disclosure of patient information outside of a "need to know"

STANDARD ACCOUNTINGS MUST INCLUDE:

- Date of disclosure
- Name of recipient and address if known
- Brief description of the PHI disclosed
- Brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for disclosure or copy of the request for disclosure.

*Note

Individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment or to persons involved in the individual's health care.

OMNIBUS BREACH

A *breach* is generally an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. 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 PHI has been compromised.



OMNIBUS BREACH, CONT..

Examples of PHI Breach:

- Misdirected faxes containing PHI
- PHI provided to the wrong requester
- PHI given without authorization
- Inappropriate disclosure to employer or co-worker
- Identity theft
- Theft of and disclosing PHI
- Lost sensitive information (media or paper)
- Inappropriate access - Violates Minimum Necessary
- Confidential Communication Violations



*Note

In the event of a suspected breach of PHI, The HIPAA Privacy Officer must be notified immediately.

HIPAA SECURITY RULE

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

Examples:

- Unique User ID's
- Complex Passwords
- Automatic Log-Off After Period of Inactivity
- Annual HIPAA Training (required by NYTPS)



*Note- Medical records are a prime target for Cybercriminals

- Medical ID Theft
- Medicaid/Medicare Fraud
- Credit Card Fraud
- Other Financial Fraud



SECURITY RISKS

REDUCED BY A “CULTURE OF COMPLIANCE” or
FOLLOWING YOUR POLICIES AND PROCEDURES



➤ SECURITY IS 25% COMPUTER SECURITY



➤ 75% USER BEHAVIOR

SECURITY RISKS, CONT...

CYBERSECURITY AWARENESS



- THINK TWICE BEFORE CLICKING
- NEVER DISABLE SECURITY CONTROLS SUCH AS ANTI-VIRUS, FIREWALLS OR OTHER PROTECTIVE 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 PHI SHOULD BE PLACED “FACE DOWN”.
- WHEN YOU LEAVE YOUR WORKSTATION, PRESS “CONTROL L” (locks)
- DO NOT THROW AWAY PAPER WITH PHI. (check for phi on “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

CRITICAL SECURITY PROTECTIONS

COMPLEX PASSWORDS CHANGED EVERY 90 DAYS

A strong password is a combination of numbers, uppercase letters, lowercase letters, and, if possible, other characters. This makes the password nearly impossible to guess in a reasonable amount of time, and ensures that all the hard work you put into keeping your machine well-defended does not go to waste. The longer the password, the harder it is to guess.

GUIDELINE FOR CREATING STRONG PASSWORDS:

- Be 8 characters or longer
- Use a combination of upper and lowercase letters and
- Include at least one numeric and/or special character (& ? @) punctuation and spaces
- Do Not cross passwords. Use separate passwords for work and home

*Note

BRUTE FORCE ATTACKS CAN TRY THOUSANDS OF COMBINATIONS PER SECOND

-4.7% OF USERS HAVE THE PASSWORD "PASSWORD"

-91% HAVE A PASSWORD FROM THE TOP 1000 PASSWORDS

-TREND PASSWORDS ARE COMMON



CRITICAL SECURITY PROTECTIONS

EMAIL AWARENESS AND SECURITY

ALWAYS VERIFY THE EMAIL ADDRESS TO THE LETTER

DO NOT OPEN ATTACHMENTS – UNLESS:

- You expect the email with the attachment
- Have verified the attachment was sent by a trusted source



***Note – WEB BROWSING DANGERS**

- Visiting an infected website can download malicious software to your network
- Only use the web for work-related purposes, even on your own time, to protect PHI



CELL PHONE DANGERS



- CAMERA FOR IMPROPERLY RECORDING PHI
- EASILY LOST, STOLEN OR DISCARDED WITH PHI
- ACCESS TO EMAIL AND TEXT MESSAGING WITH PHI
- EASY ACCESS TO SOCIAL MEDIA FOR IMPROPER POSTING OF PHI
- MICROPHONE AND CAMERA ACCESSED AND TURNED ON
- USB CONNECTIONS PERMIT UNAUTHORIZED FILE TRANSFER

*Note – IMPLEMENT SECURITY MEASURES TO REDUCE CELL PHONE RISK

- Disable connectivity to unsecure Wi-Fi, Bluetooth, cloud storage or file sharing network services
- Add anti-virus/malware to your mobile device
- Review apps or games for their access to all data on your phone
- Verify apps only have minimum necessary permissions required

PROTECTING PATIENT PRIVACY

EVERYONE'S RESPONSIBILITY

1. PROTECT THE PATIENT FROM THE HARM A BREACH COULD CAUSE
2. MAINTAIN THE REPUTATION OF YOUR PRACTICE



VERBAL COMMUNICATION

When talking about confidential information make sure you are:

- Sharing only with someone who needs to know the information to perform their job.
- Giving only the minimum amount of information necessary.

When talking about confidential information be aware of your surroundings.

- Avoid discussing PHI in public areas such as cafeterias or elevators, etc.
- When conversations in open areas cannot be avoided, remember to keep your voice low.



TIPS REGARDING PHI

- Review information before sending to make sure you are sending **ONLY** what is necessary.
- Double-check the email address or fax number.
- Always use a fax cover sheet with Confidentiality Notice
- Email scanned documents to yourself before e-mailing them to the final recipient.




TIPS TO DETERMINE IF YOU CAN USE OR SHARE PHI:

- 1) Is the disclosure for treatment, payment or health operations purposes?
- 2) If not, do you have written authorization from the patient?
- 3) If not, is there another legal requirement for disclosure?

PROTECTING ELECTRONIC DATA – FOLLOW UP

Confidential information stored on computers and other electronic devices requires special measures to keep it private.

To protect confidential information stored as electronic data, you should:

- Avoid internet threats.
 - Ensure data is encrypted.
 - Use social media and blogging sites appropriately
 - Create strong passwords
 - Secure computers and other mobile devices
- 

ENCRYPTION

What is Encryption?

Encryption makes electronic data (on computers, mobile devices such as laptops and smart phones) unreadable. Only authorized users of the data will have a key to “unlock” the encryption.



SECURITY FOR MOBILE DEVICES – FOLLOW UP

Any mobile device with confidential information on it should be encrypted. If not able to be encrypted (i.e. camera) it should be physically secured when not in use in a locked drawer or safe. Make sure you know where these devices are at all times.

Some common mobile devices:

- Laptops, Tablets
- Smart Phones, Cell Phones
- Flash Drives, Memory Cards, CDs/DVDs, External Hard Drives
- Cameras



***Report any loss or theft of a mobile device containing confidential information to your computer support center immediately.**

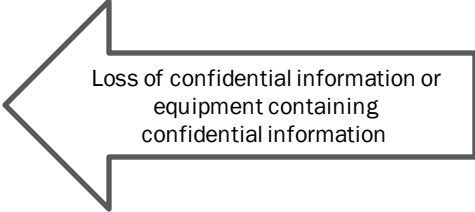
REPORTING PRIVACY AND SECURITY VIOLATIONS

Issues that should be reported:

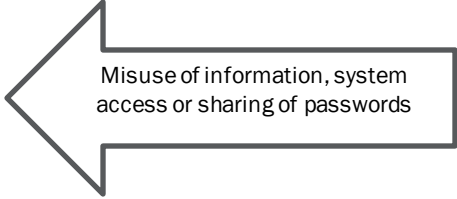
- Stolen laptop
- Lost smart phone
- Misplaced patient documents

- Sharing of passwords

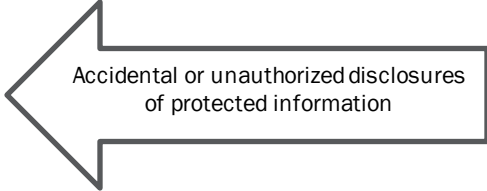
- Misdirected faxes and email
- Human error
- Overheard conversations
- Inappropriate social media posts.



Loss of confidential information or
equipment containing
confidential information



Misuse of information, system
access or sharing of passwords



Accidental or unauthorized disclosures
of protected information

SPECIAL REPORTING REQUIREMENTS FOR SOCIAL SECURITY NUMBERS

The confidentiality of Social Security numbers has special legal protection.

If social security numbers are released or disclosed to anyone who does not have a need to know them to perform their job, this must be reported immediately.



THANK YOU



Questions? Contact Katherine Mollberg, Compliance Coordinator:
631-473-4284 Ext 153
katherine.Mollberg@nytps.com