



E4 Employee HIPAA Training

The Health Insurance Portability and Accountability Act of 1996
Dept of Health and Human Services
Office of Civil Rights (OCR)



What is HIPAA?

- The intent of HIPAA is to protect clients, reduce fraud, improve quality of health care, and set strict standards for how private information about clients is transmitted... HIPAA, 1996).

http://counselingoutfitters.com/vistas/vistas08/Freeburg_Article_29.pdf

- To make the electronic transfer of health information more efficient, HIPAA establishes new uniform standards for sharing that information. HIPAA provides new federal requirements (HITECH Act) to ensure the confidentiality and privacy of health information, given the federal mandate for Electronic Health Records (EHR) by 2015. Under HIPAA, health plans and health care providers that transmit in electronic format must maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of health care information. BA's (Business Associates) have the same provisions as the Covered Entity.
- **It is important to remember that one of HIPAA's main purposes was to provide greater rights and protections to health care patients. So, whichever law does that - HIPAA or a particular State law – trumps. In addition, patient consent for release of mental health and substance abuse treatment is still required.**

HIPAA Is For Everyone

- Everyone at E4 Health is mandated to comply with HIPAA laws and PHI protection.

This includes:

- Counselors (MA II, MA III)
- Account Services
- Finances
- Administrative Staff
- Training Staff
- Management at all levels
- Vendors with access to E4 PHI
- Cleaning staff
-



Basic Vocabulary

Covered Entity – Any healthcare organization which has access to protected health information. E4 Health is a ‘covered entity.’

PHI – Protected Health Information - *Generally, PHI is any information about health status, provision of health care, payment, and medical records (HIPAA, 1996)*

Privacy Rule - The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to ... and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. Covered Entity (E4 Health, Inc.) may not use or disclose PHI, except as permitted or required by Privacy Rule.

Security Rule – Three specific types of security safeguards: administrative, physical, and technical.
Electronic Communications are part of the Security rule

More on PHI

PHI (Protected Health Information) includes:

- Health information, including demographic information
- Relates to an individual's physical or mental health or the provision of or payment for health care
- Identifies the individual

PHI applies to any Protected Health Information which is transmitted or maintained in any form or medium by a Covered Entity (E4 Health – our phones, email, database) or its Business Associate (WPO, TCS (database company), CLC, etc.



Client Rights

- May request a copy of his/her records (PHI)
- Administrative information
- Email sent to QI for request
- Client's record is documented with a Client Inquiry note
 - Special ROI form, requiring a Notary Public witness and stamp
- Right to complain
- Right to know about non-routine disclosures (breaches)
- Right to alternate communications (phone, snail mail, etc)
- Right to request amendment/correction

Client Responsibilities

- Providing accurate information
- Ethical behavior
- Read and sign Notice of Informed Consent (if possible)
- Phone counseling: Review and refer member to website to see and/or download full HIPAA Statement of Privacy Practices – www.LifeScopeEAP.com and www.moretolifeonline.com
- Let us know how best to communicate with him/her
- Let us know any restrictions or exceptions of PHI

E4 Employee Responsibilities

- Make sure doors close and lock
- Keep PHI printer/PHI fax room doors closed
- Ensure all PHI at printer & fax rooms without doors is contained and then shredded after use
- Secure PHI
- Secure computers
- Immediately report non-compliance to your supervisor for investigation
- Don't discuss clients in public areas
- Read Confidentiality Statement to each caller
- Keep it simple:
 - 'Need to know' rule of thumb

Daily Procedures



Screen and sign-in
visitors



Always lock
computers when
away from desk



Do not leave PHI
materials in plain sight



Face computer
screen away from
unauthorized visitors



PHI is always
shredded after use



Make sure doors
close and lock

More Technology



Cell Phone protection

Ensure phones have a password if you have access to E4 email



Cell phone cameras – turn off phones in work areas



Cloud Storage - This is against company policy.



USB ports - These have been disabled on all computers



Email encryption

Auto encrypt any outbound email suspected to have PHI



Computers on idle > 5 minutes will 'lock' automatically

End of Day Checklist



Turn off computers



Desks and file cabinets
locked



File all PHI within locked
cabinets



Remove all PHI
materials from fax, copy,
and printer machines



Shred any hard copy PHI
laying around

Working from Home

- All the same rules apply at home as in the office
 - *Turn off computers*
 - *Desks and file cabinets locked*
 - *File all PHI within locked cabinets*
 - *Remove all PHI materials from fax, copy, and printer machines*
 - *Shred any hard copy PHI laying around*
- Work in separate space from rest of household
- Treat company property with respect and care

E4 Clinicians Guide

An E4 Clinician, Finance, Account Services and/or Management employee can discuss or release PHI without written permission from client:

- ✓ For treatment activities of any health care provider
- ✓ For payment activities of any health care provider
- ✓ For healthcare operations. Healthcare operations includes:
 - › Quality assessment and improvement activities
 - › Training, accreditation, certification, credentialing, licensing, reviewing competence, evaluating performance
 - › Fraud and abuse detection

Treatment activities include:

- ✓ Providing, coordinating or managing health care; consultations among health care providers; referrals of patients from one health care provider to another

Electronic Transmission of PHI

- Never send PHI in the body of an email unless communicating directly with the client, with the client's permission
- If you send email containing PHI from E4 Outlook or HealthMap, it will be automatically encrypted.
- **Always** include the confidentiality notice in your email signature
- When faxing, make sure your fax is going to a secure fax and someone is there to receive it.
- **DO NOT SEND EMAIL FROM NON-E4 EMAIL ADDRESS. EVER...**

Transporting PHI

- No PHI should be removed from the building without signing an agreement with their department Vice President
- Do not email PHI to your personal home email address
- Vehicle transport of PHI
- Two lock rule
- Flight transport of PHI
- Always keep PHI with you
- Please review the E4 policies under Technology Documents in Sharepoint
- <https://sharepoint.e4healthcare.com/tech/Shared%20Documents/Forms/GroupByClassification.aspx>

HIPAA Compliance



Site visits conducted



Internal monitoring by
management



Create work plans for
each worksite



Ongoing Policy &
Procedures Development
as we grow



Implementation of work
plans and P&P

HIPAA Sanctions – Beware!

- **CVS Pharmacies:** \$2.25 million for throwing out hundreds of used prescription bottles with patient labels on them.
- **UCLA Health System:** \$865,000 fine for improper celebrity chart access (plus individuals involved were charged with federal misdemeanor charges)
- **Howard University Hospital:** Laptop stolen from contractor with PHI of almost 35,000 patients. Contractor (now ex-contractor) had downloaded the data to personal laptop in violation of hospital policy. Personal laptop unsecured and unencrypted
- **Randi A.J. (Anonymous) v Long Island Surgi-Center:** a patient requested she only be called on cell phone, not home phone. A nurse called home phone and discussed the case with the patient's mother. Patient sued. Result: Appellate Court found gross disregard of patient's right to the privacy and confidentiality of sensitive medical information – and patient was awarded financial damages payment.

HIPAA Penalties

Internal Sanctions

Work in progress

Civil Penalties

\$100 per incident, up to
\$25,000 per year per person
standard

Federal Criminal Penalties

Up to \$250,000 and/or up to 10
years in prison for knowingly
and improperly disclosing or
obtaining protected health
information

Workstation Requirements

Is my desk in my sight? If not:

- Lock your computer screen (Windows icon and L)
- Turn off your computer screen
- Lock up PHI at your workstation
- All filing cabinets locked at end of day
- All PHI materials removed from fax, copy & printer machines
- All PHI which isn't needed is shredded



Officers

HIPPA PRIVACY OFFICER

Bara Litman Psy.D., CEAP, VP Account Services

972-810-3054

617-435-7326 (cell)

Bara.litman@e4healthcare.com

HIPPA SECURITY OFFICER

Ameet Patel, MBA, VP IT and Support Services

972-810-3040

Ameet.Patel@e4healthcare.com



“If in doubt, assume it’s PHI.” Ameet Patel

HIPAA

“It is everyone’s responsibility and critical to our business success. Compliance with Privacy and Confidentiality represents one of our core competencies.”

–Bill Mulcahy and Cindy Sheriff

