NATIONAL CONSORTIUM OF
TELEHEALTH
RESOURCE CENTERS

HIPAA & Telehealth

A Stepwise Guide to Compliance

Should I Be Concerned?

STEP 1

DOES HIPAA APPLY TO ME AND MY TELEHEALTH PRACTICE? HIPAA applies to you if you are a healthcare provider that transmits personal health information (PHI) in electronic form. If you do, you ARE a covered entity (CE).

STEP 2

IS THE INFORMATION I AM TRANSMITTING CONSIDERED PHI? Anything that can be used to identify an individual is potentially PHI. There are 18 types of identifiers considered PHI. Examples related to telehealth include names, phone numbers, birthdates, IP addresses, email addresses, device identifiers, and photos/images.

STEP 3

DO I HAVE BUSINESS ASSOCIATES? A business associate is anyone who creates, receives, maintains or transmits PHI on your behalf; or has the ability to come in contact with PHI in your practice. See PHI examples above.

OK, NOW I'M WORRIED! Keep Reading To Find Out What You Can Do!

Did You Know?

#1 If you are sharing any type of PHI with Business Associates, any mistakes they make in protecting the security and privacy of your data are yours too. YOU are still responsible.

#2 Your compliance is now dependent on their practices.

#3 You can protect yourself by having formal Business Associates Agreements (BAAs) documenting how they are protecting your PHI and by performing reasonable due diligence to verify their security practices.

Do not disclose PHI to any Business Associate unwilling to sign a BAA.

Complying With HIPAA

HIPAA compliance is a combination of physical, administrative and technical safeguards. Technology alone cannot be HIPAA compliant or make you HIPAA compliant. Here are the things you and your Business Associate(s) should do and document:

RISK ASSESSMENT: Conduct a comprehensive review of where you store or access PHI and how secure it is in each case. Take appropriate steps to secure it in a way that fits for your organization. Establish and document your security policies and procedures. Train your employees regularly and consistently.

INFORMATION SYSTEMS ACTIVITY REVIEW: Conduct and document periodic reviews of access logs or other records for unauthorized activity. It might be bad news if you find some, but YOU want to be the first one to find it. Report the breach and implement a fix immediately. Confer with counsel about what to do next.

You might also want to consider ways to configure your system so that PHI is not stored or shared.

4 Questions to Ask a Potential Business Associate

...but they all say they are HIPAA compliant...

Question 1:
Which of the 18 identifiers of PHI would your company be CAPABLE of accessing?

Question 2:
May I view the results of your last HIPAA compliance audit?

Question 3:
What administrative, physical and technical safeguards do you have in place?

Question 4:
Would you be willing to sign OUR BAA?

Extra Credit Compare these measures among vendors!

Note to Self... Encryption alone is not compliance, and processes that are compliant in a clinic-to-clinic encounter may not be compliant in a clinic-to-consumer encounter. Context matters.

Things to Keep In Mind WHEN (not IF) You Have a Breach...

What Is At Stake?

Financial Penalties

WILLFUL NEGLECT VIOLATIONS
"But You Did Know*"

Corrected in required time period < Uncorrected

$10,000+ per violation - **$50,000+ per violation**

*Requires only knowledge of the actions that constitute an offense. Specific knowledge that a particular action violates the HIPAA statute is not required.

Fines + Criminal + Civil Penalties

The Maximum Penalty is $1.5 Million Per Year Per Violation

Learn More About HIPAA

* HHS Office for Civil Rights
* Center for Connected Health Policy
* Electronic Code of Federal Regulations
* HIPAA.com
* UMTRC HIPAA Clarifications
* NIST HIPAA Security Rule Toolkit
* American Medical Association and HIPAA

Have questions? Contact a Telehealth Resource Center!