PERSON
CENTERED
TECH

Risk Management in Group Practice

HIPAA Security & Technology

Objectives

- Identify what forms of HIPAA Security policies and procedures are necessary for a group practice's compliance
- Choose an employment structure that supports HIPAA Security compliance

Q1: How Do You Comply With HIPAA Security?

3 Steps to HIPAA Security Compliance

Easy peasy!

1. Do a Risk Analysis
2. Make a Risk Mitigation Plan
3. Write your Security Policies and Procedures

Why Policies?

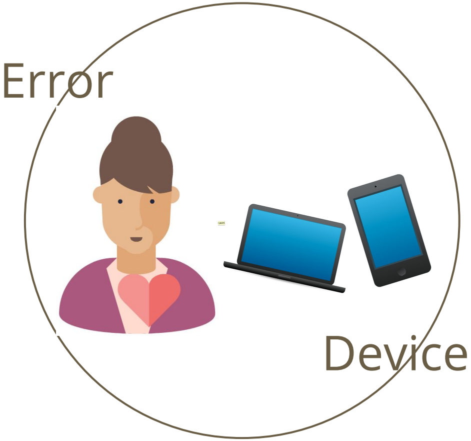
- Documentation or it didn’t happen
  - Documentation is what you *did*
  - Policies are what you *do*
- A solo practitioner need only look after herself. A group must rely on everyone to keep the practice and its clients safe
- Policies keep you and the practice on-track
- The HIPAA Security Rule requires the practice to have policies and procedures that describe how the practice complies with each of the Security Rule’s standards. See them here→

Q2: What’s Different About HIPAA Security for Groups?

Risk "Surface Area"

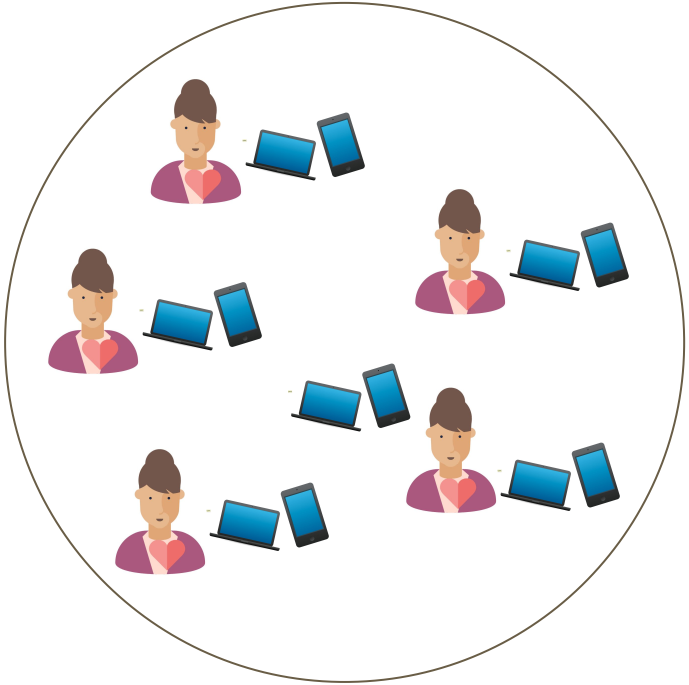
Internet Risks

Human Error



Device Risks

Solo Practice



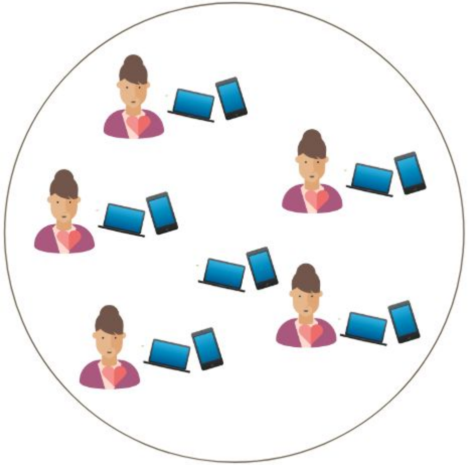
Group Practice

“Bring Your Own Device”

Most groups rely on clinicians to use their own equipment in the practice

- Reduces costs
- Clinicians usually prefer it this way
- Sounds great!

Imagine the risk surface area image, but the devices could all be any kind and you have no real control over how they touch practice systems or information.



Bring Your Own Device Policies

- Policy should define:
  - How personal devices must be secured
    - Includes technical stuff (settings, configurations)
    - *and* how devices are handled (behaviors)
  - Acceptable use for personal devices
  - Acceptable apps for personal devices
  - How the practice reimburses (or doesn’t) for costs of personal device usage
- There should be an audit process for personal devices
  - Larger organizations often require people to install device management software on personal devices

“Workforce”-Related Policies

- “Workforce”: People who work in the practice under its policies and procedures
  - Business Associates work under their own policies and procedures
- Sanction policy
  - Many HR policy sets already have this
- Training Schedules
- Onboarding and offboarding procedures
- Procedures for deciding what information and facility access each workforce member needs

Q3: Should I Go With Independent Contractors or Employees?

What's the Difference?

Contractor pay doesn't require all those extra employer taxes

Contractors can be required to take care of a lot of their own needs

HIPAA Security and Contractors?

HIPAA doesn’t care about tax-related designations like “contractor” and “employee.” It just cares about “Workforce” vs. “Business Associate.”

But…

Can you require contractors to comply with all your security policies and procedures without violating employment law?

References

- US Dept. of Health and Human Services. (2006). HIPAA Administrative Simplification . Washington, DC: Author.
- US Dept. of Health and Human Services. (2013). HIPAA Omnibus Final Rule . Washington, DC: Author.