

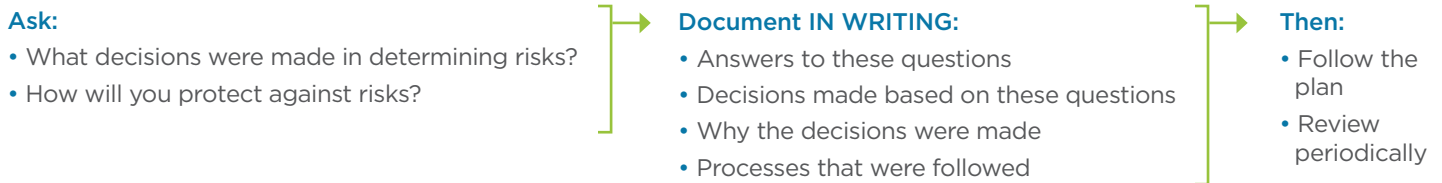
WEBINAR TAKEAWAYS: THE HIPAA RISK ASSESSMENT



What is the purpose of the HIPAA Risk Assessment?

- **Required** to ensure that an organization is compliant with HIPAA's **administrative, physical, and technical** safeguards.
- **Identifies** where ePHI is being used and determines how breaches of ePHI security could occur → **The actual process you follow when identifying these risks is just as important as protecting against the risks.**
 - **What is the ePHI?**
 - **Who may need to access the ePHI?**
 - **What systems does the entity have that will require protection?**
- **Provides** the roadmap for what security measures a covered entity needs to have in place

What is the Risk Assessment process?



Identify where & how PHI is:

- Created
- Received
- Maintained
- Processed
- Transmitted

Consider:

- Cell phones
- Removable media (flash drives)
- Telecommuters
- Copy machines
- Databases
- HRIS systems
- Payroll systems

Identify current security measures.

- Are they being observed?
- How effective are they?

Identify threats.

- Theft
- Hacking
- Human error
- Human mischief
- Failure of organizational resources (i.e. improperly maintained/ configured hardware or software)
- Natural & man-made disasters

Identify vulnerabilities.

- **Poor building security** = ePHI exposed to theft
- **Bad coding** = ePHI exposed to hacking
- **Inadequate access controls** = ePHI exposed to human error / mischief
- **Failure to install software updates** = ePHI exposed to failure of organizational resources
- **Poor data backup practices** = ePHI exposed to loss through natural or man-made disasters

Assess the likelihood that a particular threat will exploit a given vulnerability.

- **Your organization's experience:** What will you actually experience in the course of conducting business?
- **Similar organizations:** Examine other companies similar to yours.
- **Organizations using similar systems:** Ex: Lotus Notes, Outlook, Peoplesoft, etc.

Where do potential risks exist?

Unauthorized Acquisition of ePHI

- Laptops
- Hacked databases

Risks to data integrity & availability

- Unauthorized modifications
- Accidental errors
- Omissions
- Unauthorized/inadvertent creation or deletion

Natural disasters

- Floods
- Earthquakes

Environmental Threats

- Fire
- Power Outages
- Equipment failure/ obsolete equipment

The Security Rule requires an analysis of these threats, typically called a **Contingency Plan or Disaster Recovery Plan.**