

HIPAA Security Rule Training

Greater Kansas City Dental Society

June 4, 2019

Presented by David Holtzman, JD, CIPP

Executive Advisor, CynergisTek

Today's Presenter

- Executive Advisor, CynergisTek, Inc.
- Subject matter expert in health information privacy policy and compliance issues involving data protection and breach notification standards
- Experienced in developing, implementing and evaluating health information privacy and security compliance programs
- Former senior advisor for health information technology and the HIPAA Security Rule, HHS Office for Civil Rights



David Holtzman
CynergisTek, Inc.

Agenda

- Objective
- HIPAA Security Rule Basics
- Password Management
- Malicious Programs and Incidents
- Log-in Monitoring
- Security Reminders
- Security Best Practices

Objective:
To Create
awareness on
best practices
required to
protect
information
and assets

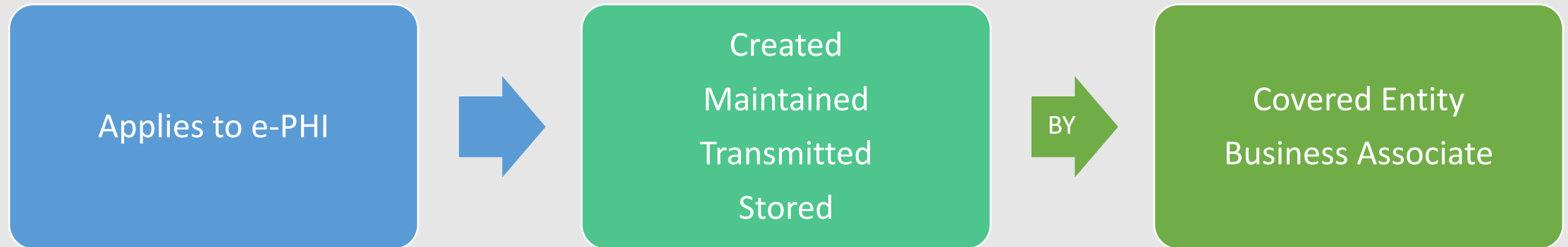
The **HIPAA Security and Awareness Training** standard requires an organization train all members in their workforce on its security policies and procedures and includes the following implementation specifications:

- **HIPAA Security Rule Basics**
- **Password Management**
- **Protection from Malicious Software**
- **Log-in Monitoring**
- **Security Reminders**



HIPAA Security Rule

Scope of HIPAA Security Rule



The Guiding Principles of Security Rule

- Ensure e-PHI is used, stored, transmitted or received with:
 - **Confidentiality**
 - Only the right people see it
 - **Integrity**
 - The information is what it is supposed to be – no unauthorized alteration or destruction
 - **Availability**
 - The right people can see the e-PHI when needed

Goals of HIPAA Security Standards

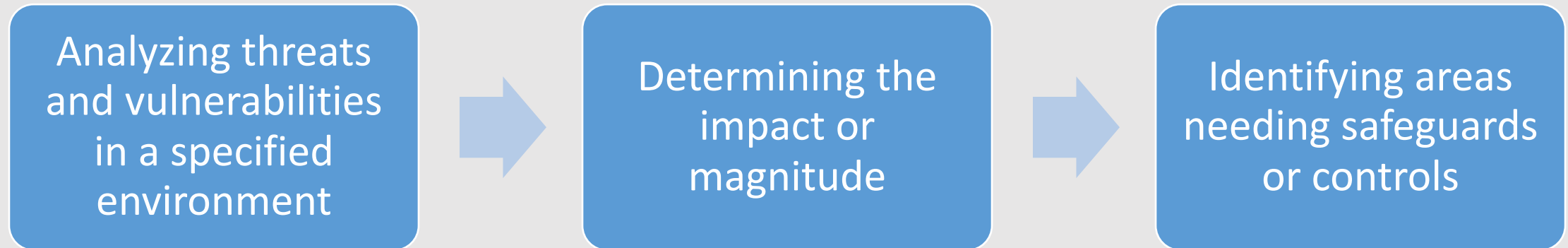
- Protect e-PHI against reasonably anticipated threats or hazards to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by the Privacy Rule
- Establish policies, procedures and training to ensure compliance by workforce
 - Administrative Standards
 - Physical Standards
 - Technical Standards

Risk Assessment

- An assessment of threats and vulnerabilities to information systems that handle e-PHI.
- This provides the starting point for determining what is appropriate and reasonable.
- Organizations determine their own technology and administrative choices to mitigate their risks.
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment.
- For additional information:
<https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es>

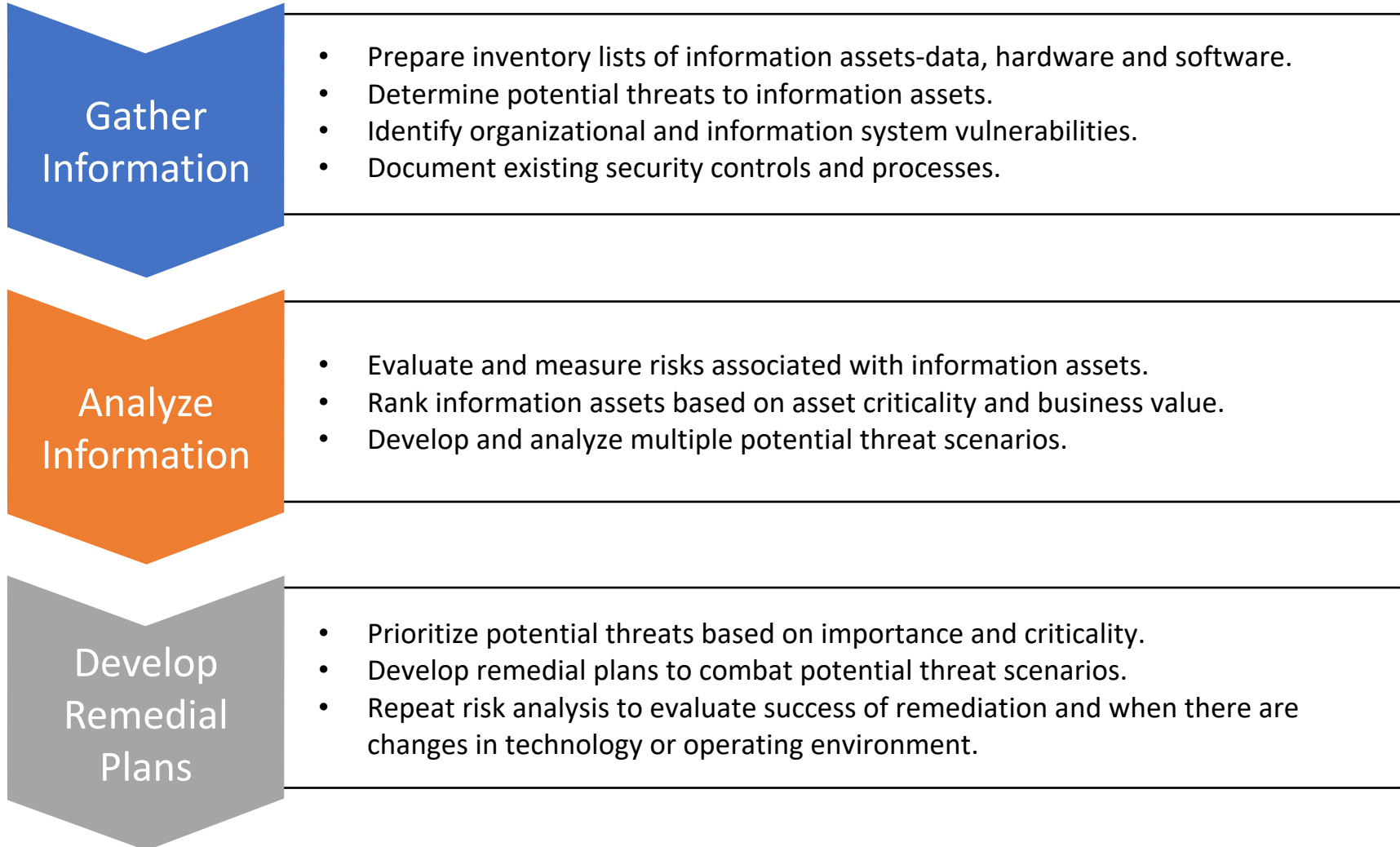
What is Risk Assessment?

The process of:



For additional information: Security Risk Analysis Tool <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

Performing a Risk Analysis



For additional information: <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>



Password Management

Protecting Against Internal Threats: Passwords

- Do not share – never give a password to someone else
- Use strong passwords for your network account and any other applications.
 - Create a password with a minimum of 8 characters
 - Your password should contain at least three of the following four components:
 - Uppercase Letters (A B C D)
 - Lowercase Letters (a b c d)
 - A Number (1 2 3 4)
 - A Special Character (% , ^ , * , ! , ?)
- Change your password regularly – at least every 90 days.
- You cannot reuse the last 5 generations of a password.
- Change your password immediately if you think it is compromised!
- For additional information refer to: <https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication>



Password Security

- Choose a secure password
- Don't write it down anywhere near your computer, place it in a secure location
- Log-off or lock your workstation when leaving your desk

Password Security User Responsibilities

- Change passwords often
- Don't use the same password for multiple accounts
- Don't email or share your password with others
- Do not store or embed your password in shortcuts or scripts

Unauthorized Access

- Unauthorized access includes but is not limited to the following:
 - Sharing your system login information for another's use
 - Using someone else's login information to access systems
 - Accessing information that is beyond your "need-to-know" or not within your role
- You are always responsible for securing your login information (credentials such as user IDs, passwords)
- Do not share your credentials

User Responsibilities When Sending Email

- Review Attachments
- Double Check Addresses
- Use Encryption with Confidential Data
- Do Not Use Personal Accounts
- Do Not Share Your Password
- Remember That All Emails Are Saved
- For additional information: <https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-store-sensitive-personal-information-securely>



Malicious Programs & Protections

Malicious Programs

- These programs pretend to be legitimate. Their objective is to fool the user into installing them. Then the computer or information system gets infected.
- Malware often comes disguised in email messages that invite you to click on a hyperlink to access another website or download a file to your computer
- This is often called Phishing
- Do not download or install programs in your computer.
- Allow trained IT personnel to evaluate, install and configure applications that are authorized by the dental practice.

- For additional information refer to: <https://www.ftc.gov/news-events/blogs/business-blog/2018/11/cybersecurity-small-business-phishing>

Malicious Programs

- Malicious programs invade the computer and are difficult to identify. These programs can come through:
 - Email
 - External media (USB, CD, DVD, etc.)
 - Disgruntled employee installs malicious software
 - Accessing a fraudulent internet address or website
 - For additional information to:
<https://www.ftc.gov/news-events/blogs/business-blog/2018/12/cybersecurity-small-business-business-email-imposters>

Ransomware Symptoms

- Has the capacity to block the user from executing programs on their machine; all the machine presents are sites where to pay the ransom.
- Closes the programs that you're using.
- Encrypts your data to such an extent that you can't open files or applications.
- For more information:
<https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

Ransomware: How To Prevent It

- Continuous monitoring (24 x 7) of external connections to detect and block malicious and unwanted messages
- Anti-Virus and Anti-Spyware applications are in place and updated for all devices and computers that connect to your dental practice information system
- Isolation and inspection of the infected computer, to determine the type of Ransomware and avoid contamination on other computers.
- Preventive blocking of personal e-mail sites from the internal network.
- For more information: <https://www.ftc.gov/news-events/blogs/business-blog/2018/11/cybersecurity-small-business-ransomware>

A dark blue, irregular ink splatter shape is centered on a white background. The splatter has a textured, watercolor-like appearance with some lighter blue and white areas around the edges. The text "Log-in Monitoring" is written in white, sans-serif font across the center of the dark blue area.

Log-in Monitoring

HIPAA Monitoring Safeguards

- Network Protected by Firewalls
- Network Intrusion Detection Systems
- User account activity – computer use is monitored!
- Log-In Monitoring
 - Report unsuccessful log-in attempts to the IT service provider
 - IT technology may be monitoring unsuccessful log-in attempts to your account

HIPAA Violations & Consequences for Employees & Associates:

- Mandatory re-education and training
 - Corrective action plan
 - Verbal or written warning and/or documentation in HR record
 - Disciplinary action, up to termination of employment or contract
-
- For additional information refer to: <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>



Security Reminders

Security
Reminders:
Periodic
reminders to
supplement
initial HIPAA
security
training

Examples:

- A “security tip of the day” at the time of logon, or when they access the organization’s intranet.
- A “Security Awareness” column in monthly or quarterly newsletters.
- Notify users of security incidents by broadcast e-mail, including an explanation of the remedial actions that have been taken to prevent a repeat incident.
- Post interesting articles on computer security in the mailroom or cafeteria/breakroom.
- For more information:
<https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games>



Security Best Practices

Security Best Practices

- Check the authenticity of all communications. Ask before clicking a link or opening a file.
- Do not open e-mails that you are not expecting and if they are from unknown persons.
- Do not click on links or open applications attached on e-mails.
- Only visit reputable web sites.
- Do not access your personal e-mail on corporate devices.
- Do not download or install unauthorized programs.
- For more information:
<https://www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device>

Resources for Further Learning

- HHS Office for Civil Rights (OCR)
 - <https://www.hhs.gov/hipaa/for-professionals/index.html>
- HHS Office of the National Coordinator for Health IT (ONC)
 - <https://www.healthit.gov/topic/privacy-security-and-hipaa>
- Federal Trade Commission (FTC) Data Security for Small Businesses
 - <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>



Questions?

Thank you for your attention and participation

David Holtzman, JD, CIPP/G

Executive Advisor

Cynergistek

David.Holtzman@cynergistek.com

Follow me on Twitter @HITprivacy