Reducing Risk for Small Provider Practices

Bayardo Alvarez
Director, Information Technology
Boston PainCare Center
Chair, HIMSS Privacy & Security Committee
September 6, 2017
Overview

• Information Security
• Why it is important
• Challenges for a Small Practice
• Risk-based Approach
• Safeguards and Measures
• Accomplish your goals
• Lessons learned
What is Information Security?

Confidentiality

Integrity

Availability

CIA Triad
Why Cybersecurity is Important

• Millions of records digitized
• Networks are more interconnected
• Attack surface has expanded
• Cybercriminals are more sophisticated
• Federal and state regulations
• Patient privacy and patient safety
Challenges for Small Practices

• Insufficient budget
• Management on board
• Expensive technology solutions
• Multiple roles, other priorities
• Limited staff, lack of knowledge
• Malware & disaster do not discriminate
• SAME RULES & REGULATIONS
Risk-based Approach

- Prioritize systems and infrastructure
- Understand threats and vulnerabilities
- Safeguards cost/benefit analysis
- Mitigate, remediate, transfer, accept
- Repeat
Awareness & Education

• Humans introduce risks, intentionally and unintentionally
• Improve awareness, educate staff, make security a core value
• Awareness and training are cost-effective controls
• Help users understand risks: cause and effect
Filter at the Edge

- Install a firewall
- Web filtering
- Spam filtering
- Application-based filtering
Secure Endpoints

• Inventory hardware and software
• Develop a baseline security
• Run and update anti-virus software
• Implement software restriction policies
• Control access to mass media storage
• Change manufacturer default passwords immediately
• Update client devices on a regular basis, automatically
• Update infrastructure and peripherals periodically
Protect with Encryption

• In Transit
  – Wireless Encryption
  – Remote Access, Communication, Applications

• At Rest
  – Portable media (USB, external drives, tapes)
  – Portable devices (notebooks, tablets)
Harden Systems

- Disable unnecessary accounts
- Limit the functions a system performs
- Configure services & features based on role
- Firmware, OS and software up to date
- Disable unnecessary services, protocols
- Run appropriate host based firewall, anti-virus
Document & Log

• Document policies and procedures
• Network documentation and diagrams
• Hardware and software inventory
• Performance, alerts & summary reports
• Document actions, events, incidents
Prepare for Disaster

- Have a plan in writing
- Keep documentation up to date
- Alternate storage for plan, documentation
- Verify backups, restore, recovery procedures
- Keep backup media in a safe location
Accomplish your goals

• Engage management
• Strategic, tactical and operational plans
• Extend your IT staff with team “Champions”
• Team-up staff with consultants and vendors
• Security and availability must be a forethought
• Evaluate new solutions by their lifecycle cost
Accomplish your goals

- Consider outsourcing high risk systems
- Maximize built-in features and applications
- Standardize client systems and images
- Subscribe to newsletters, keep users informed
- Leverage open source, community, free tools
- Centralize documentation, reporting, alerts
Lessons Learned

- Be proactive, don’t leave it for tomorrow
- Don’t go it alone, build a team
- Security is not binary, or static
- Security is a program, not a project
- It requires more than best practices and technology