TeleHealth & TeleWork Security Fundamentals

We fear what we do not understand

BKD CYBER

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

Presenter

Nobe Aleman, CISA
Senior Managing Consultant | BKDCyber
Nashville, Tennessee
naleman@bkd.com
615.988.3589

Notification of Enforcement Discretion

- Last year, OCR exercised enforcement discretion for non-compliance during COVID-19 emergency

- https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

BKD CYBER

TeleHealth and Telework Themes

1. People
2. Processes
3. Technology

BKD CYBER

In the past & going forward

In the past:

- People come onsite to work
- Patients come to us
- Everything stays inside

Going forward:

- People work anywhere
- Patients, we “go” to them
- Everything is everywhere

Reference https://en.wikipedia.org/wiki/Medieval_architecture#/media/File:Bodiam-castle-10My8-1197.jpg & https://depositphotos.com/stock-photos/new-york-city.html?qview=11176176

BKD CYBER

TeleHealth

- 1. Asynchronous (store-and-forward): the medical information is sent health care worker and reviews it outside of real-time interactions.
- 2. Synchronous (live video and audio conferencing): real-time communication between the patient and qualified health care professional, typically telehealth.
- 3. Remote patient monitoring (RPM): patients or care providers use technology to send patients' health data to a health care worker who will assess the data

TeleHealth - People

- What do you need?
- What do your patients need?
- Training both you and patients
  - How to use technology
  - Cyber security risks

BKD CYBER

TeleHealth – People (cont.)

- Training is key for both workers and patients
  - Only 15% of healthcare professionals feel that they and their colleagues have received sufficient training in telehealth cybersecurity

TeleHealth – People (cont.)

- Patients
  - Notify patients that these third-party applications potentially introduce privacy risks.
  - Enable all available encryption and privacy modes.

TeleHealth – People (Patient)

- Is the patient who they say they are?
- Is the patient alone?
- Does the patient understand process and technology?

TeleHealth - Processes

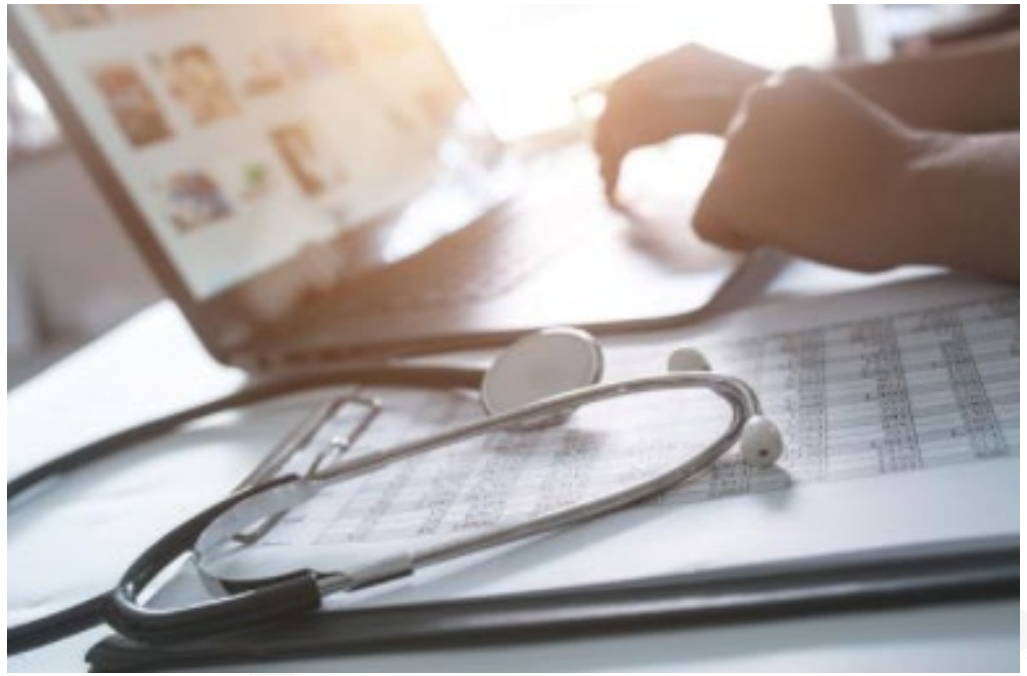
- How do you know what to do?
- How current is the policy?
- How do you educate everyone?
  - Who can champion!!!
  - Don’t put the patient and patient’s data at risk.

TeleHealth - Processes

- Monitor and review and make improvements
- In the event, the technology works; how move to another platform (e.g., phone)
- Ways to make sure the patient can’t use old version

TeleHealth - Technology

- Systems
  - Consistency, HIPAA compliance, Priorities (yours & patients)
- What to consider?
  - Simplicity, Security, and HIPAA
- Technology
  - Devices, Data, and how they meet



BKD CYBER

TeleHealth – Technology (Vendors)

- 56% of organizations suffered a breach caused by a third party
- Due diligence:
  - onboarding process
    - At a minimum, BAA & SOC2 / security equivalent report
  - “onboard” current vendors
  - Periodic review
  - Transparency

BKD CYBER

TeleWork - People

- Teleworkers who do not work securely – 90%
- Teleworkers who have did not receive IT security training after transitioning to work from home. – 73%
- Teleworkers who used personal device for work – 56%

BKD CYBER

TeleWork – People (Employees)

- Secure the workspace
- Separate work life and home life
  - What
  - Who
- Be smart and aware of threats

Reference: https://www.amazon.com/QQ-Acrylic-Keyboard-Protector-Anti-Cat/dp/B07WWBFL6J

BKD CYBER

TeleWork – Processes

- How do they know what to do?
- Develop BYOD & telework policies
  - where, when, how, what if, and the why
- What do the teleworkers need access to?
- Define policies and configure for security and don’t make it optional.
- Provide training

BKD CYBER

TeleWork – Technology (Personal)

- Tread carefully when relying on personal devices
- Manage what you can
  - Disable unsecure protocols or tools (e.g., Remote desktop Protocol)
- Limit to cloud apps with MFA.

BKD CYBER

TeleWork - Technology

- Track hardware, software, and data
- Update, Update, Update
- Make it user friendly and simple.
- Standardize hardware and images for configuration
- Remove admin access, employees should only use work device for work.
- Use single sign on

BKD CYBER

Final Thoughts And Conclusion

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

Summary

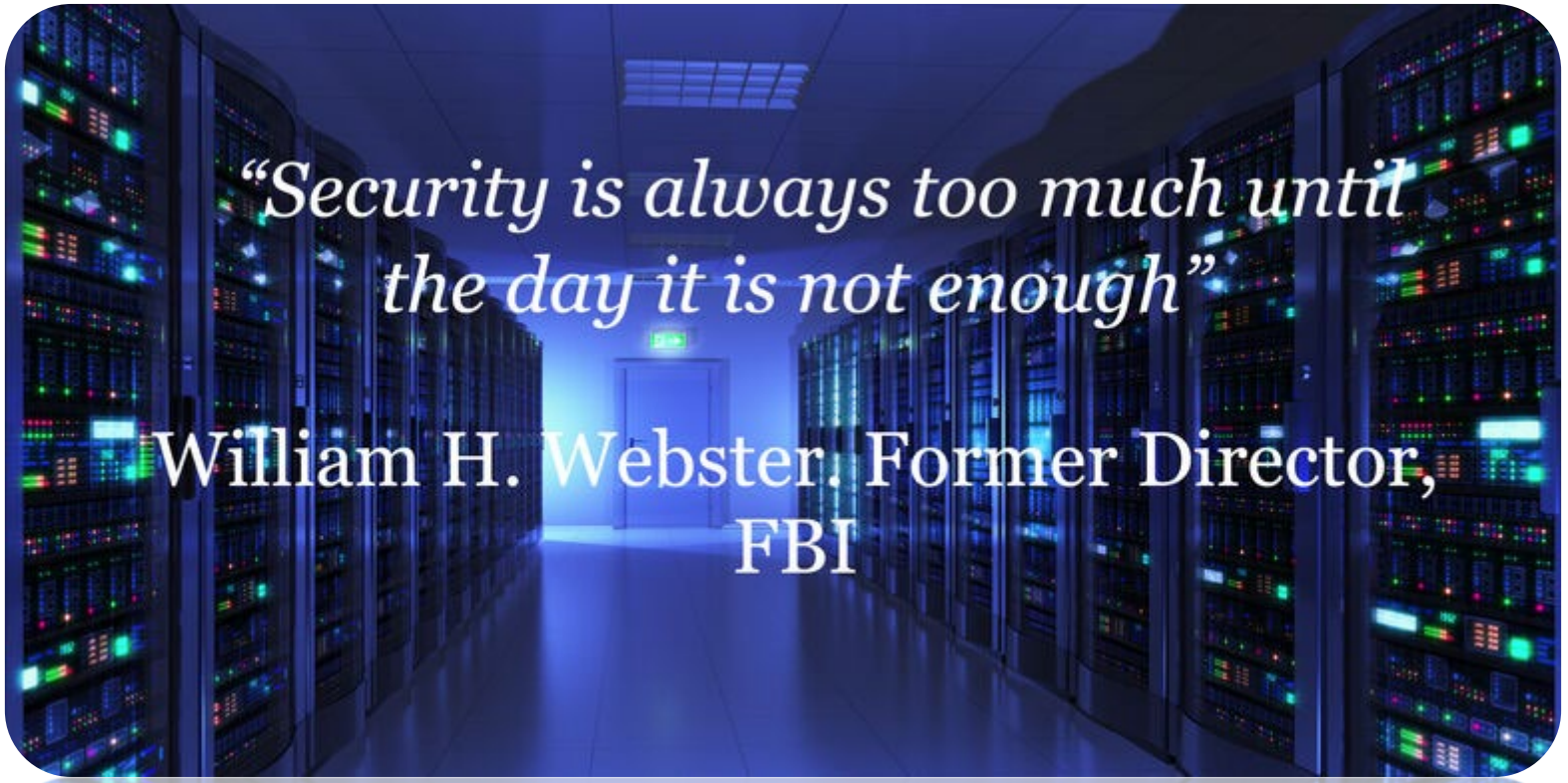
- People
  - Provide training
- Processes
  - Update, communicate, and periodically review policies
- Technology
  - Make it easy and secure
- Constantly analyze, tweak, and refine

Ending notes

- Nothing lasts forever, start looking for HIPAA compliant vendors now, the emergency provisions will eventually go away
- Look beyond compliance and start to reduce risk.
- Good Questions:
  - How do you know?
  - What do we need to do?
  - How can we better use what we have?
  - How do we know our processes are working?

BKD CYBER

A Quote to Remember!



Slides?

Questions?

Nobe Aleman, CISA
Senior Managing Consultant | BKDCyber
Nashville, Tennessee
naleman@bkd.com
615.988.3589

Thank You!

bkd.com | @BKDLLP

BKD
CPAs & Advisors