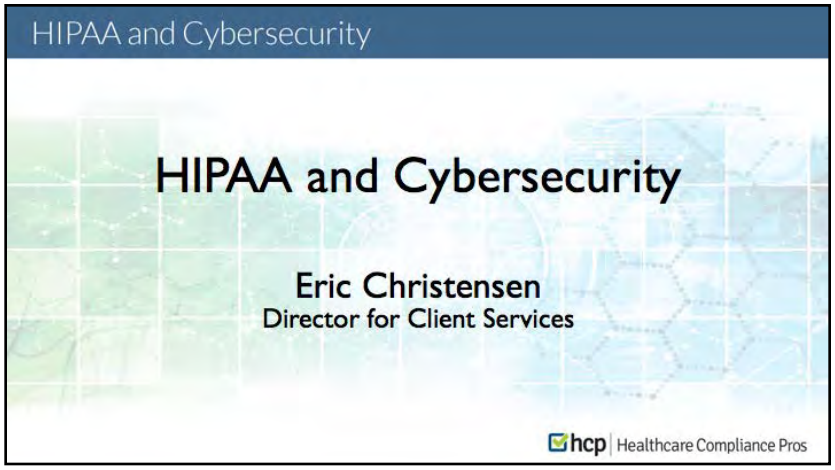
hcp | Healthcare Compliance Pros

HIPAA and Cybersecurity

Eric Christensen, Director of Client Services

Texas Orthopedic Administrators Society



SLIDE 1

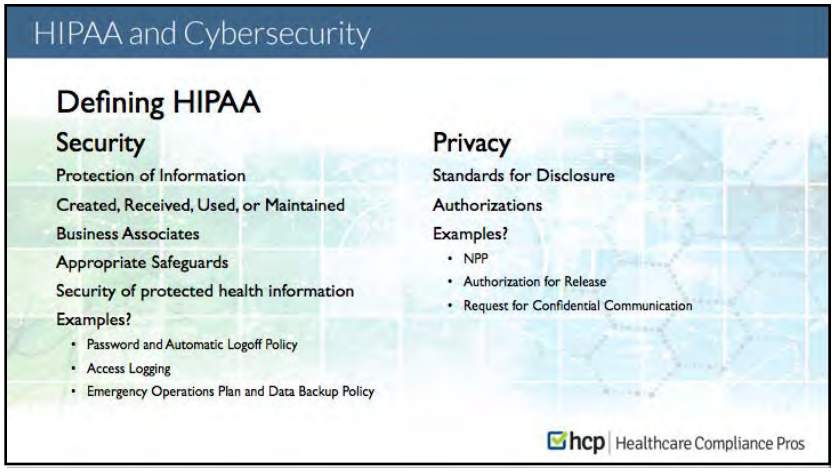
SLIDE 2

If you have a question you would rather not ask in this forum, please call or email me directly.

Eric Christensen
eric@hcp.md
801-657-4492

SLIDE 3

We'll spend just a couple of minutes defining terms.



SLIDE 4

The HIPAA Security Rule establishes national standards to protect individuals' personal health information that is created, received, used, or maintained by a covered entity, their business associates, and other downstream subcontractors.

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of protected health information (PHI).

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to Healthcare Providers.

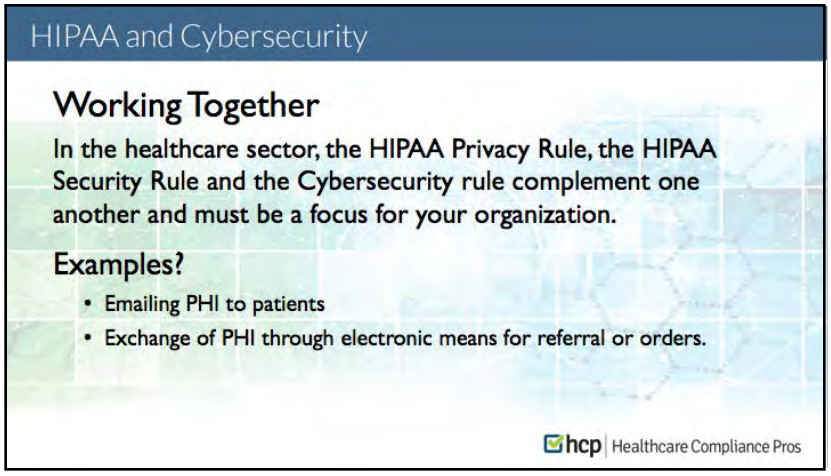
The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

SLIDE 5

On February 12, 2013, President Obama issued the "Improving Critical Infrastructure Cybersecurity" Executive Order.

Subsequently, the National Institute for Standards and Technology (NIST) published a "Framework for Improving Critical Infrastructure."

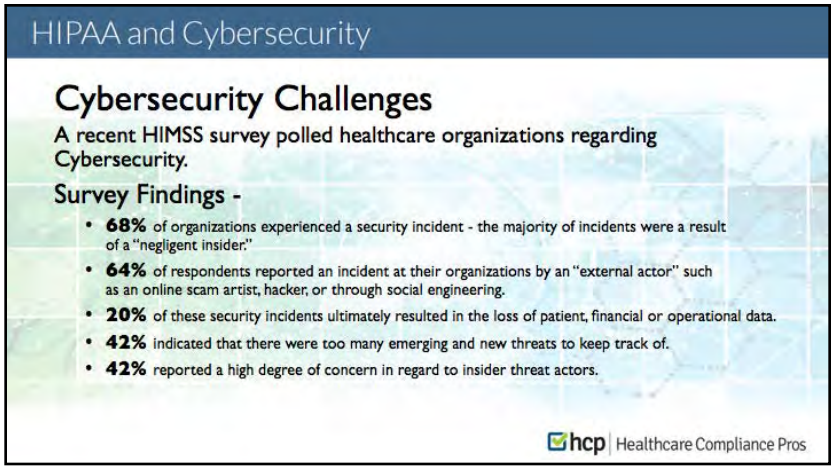
According to NIST, the Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.



SLIDE 6

Emailing PHI to patients involves their consent (Privacy), email systems (Security), external transfer (Cybersecurity).

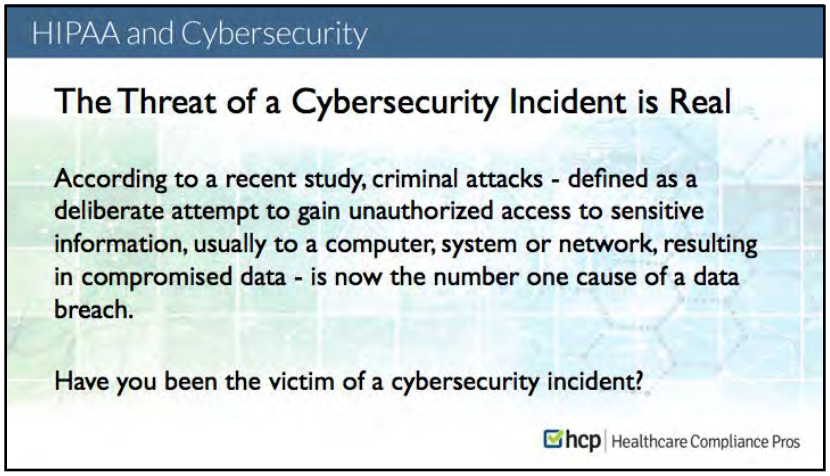
Exchange of data involves treatment (Privacy), data transfer systems (Security), and external access to data systems (Cybersecurity).



SLIDE 7

Do you understand the terminology used in the survey?

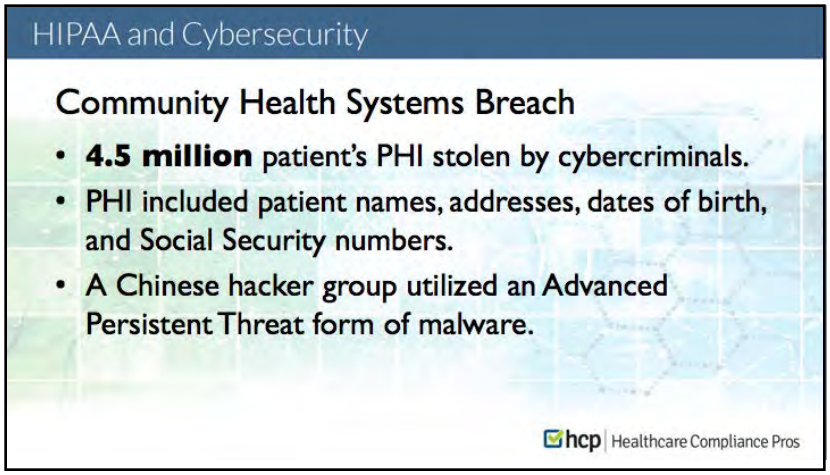
Are your organizations involved in any of these scenarios?



SLIDE 8

This can be as simple as users sharing passwords or login id's between multiple systems.

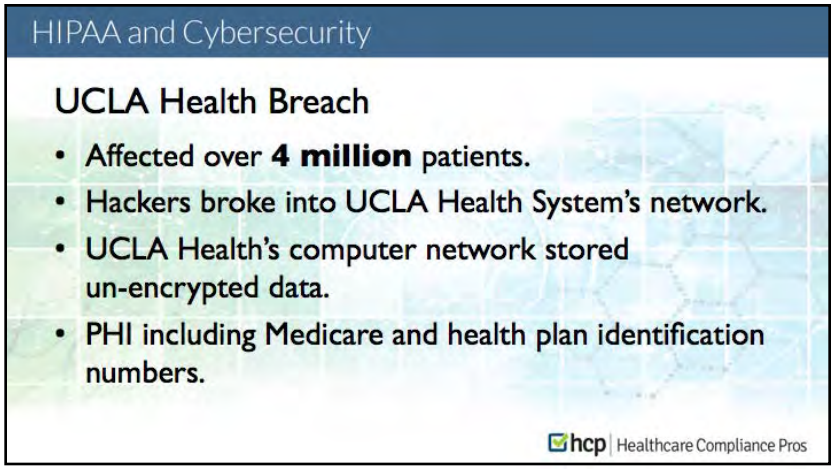
Do your physicians or employees take PHI with them on their phones, laptops, or tablets?



SLIDE 9

One of the nation's largest hospital operators notified some 4.5 million of its patients that their personal information was stolen by cybercriminals in 2014.

- Healthcare records contained patient names, addresses, and dates of birth.
- Information also included telephone numbers, insurance information, and Social Security numbers.
- To steal this information, a Chinese hacker group utilized an Advanced Persistent Threat form of malware to bypass the health care organization's cybersecurity measures.

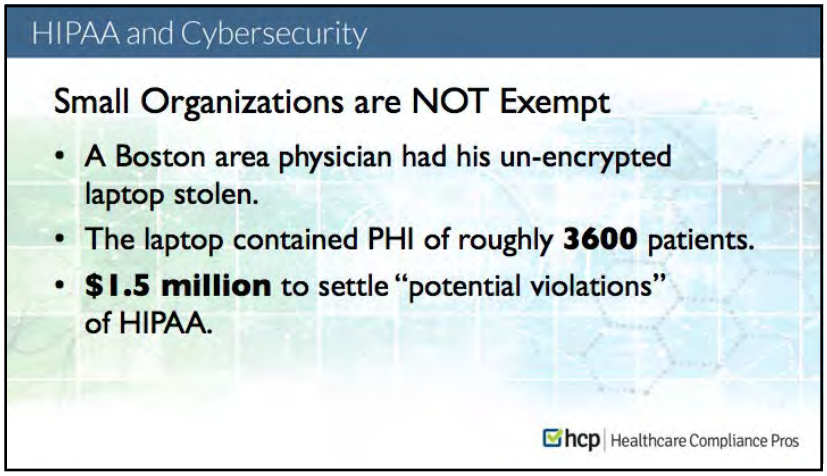


SLIDE 10

Breach affects as many as 4.5 million patients.

Hackers broke into UCLA Health System's computer network.

UCLA Health's computer network where patient information was stored contained names, dates of birth, Social Security numbers, Medicare and health plan identification numbers as well as medical information such as patient diagnoses and procedures.



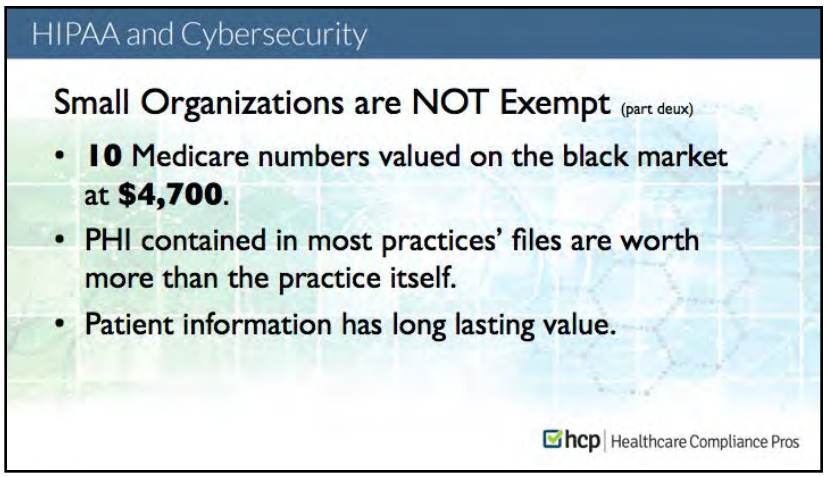
SLIDE 11

Small practices and ancillary locations are just as likely to be victim of a cybersecurity incident, especially if cybersecurity isn't a priority.

For example, a physician for Massachusetts Eye and Ear Infirmary (MEEI), a specialty hospital in Boston, had his unencrypted laptop stolen.

This laptop contained demographic and health information on roughly 3600 patients.

This breach was costly! HHS announced MEEI and an affiliated group agreed to pay the government $1.5 million to settle "potential violations" of HIPAA.

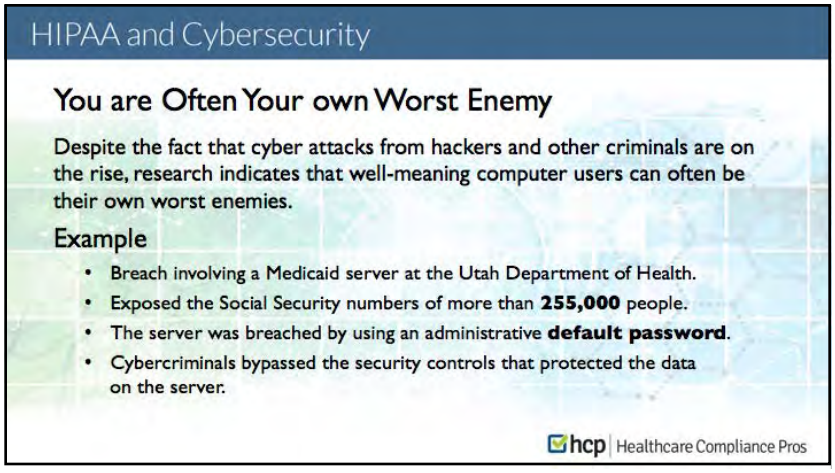


SLIDE 12

In early 2015 a bundle of information containing just 10 Medicare numbers was for sale on the black market for $4,700.

It is estimated that the information contained in most practices' PHI files are worth more than the practice itself.

Compared to credit card data patient information has a long shelf life (virtually forever).



SLIDE 13

According to several studies, we are our own worst enemies because we fail to follow basic safety principles. Whether we forget or choose not to because of lack of training, for the sake of time or workflow, or any range of reasons – not following basic safety principles is the top reason for cybersecurity incidents.

For example, a breach involving a Medicaid server at the Utah Department of Health exposed the Social Security numbers of more than 255,000 people.

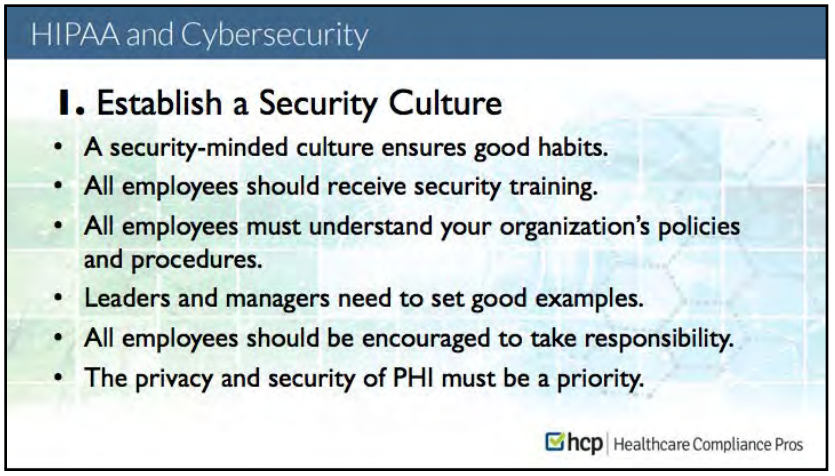
As a result, the cybercriminals bypassed the perimeter network and application level security controls that IT administrators put in place to protect the data on the server.

Have you changed your default passwords? Are your passwords easy to guess?

SLIDE 14

The U.S. Department of Health and Human Services published a list of the Top 10 Tips for Cybersecurity in Health Care. These tips were developed to help healthcare practices apply cybersecurity and risk management principles, and offer a good starting point for safeguarding health information from privacy and security risks.

I have added some additional principles to help you to ensure cybersecurity is a priority for your organization.



SLIDE 15

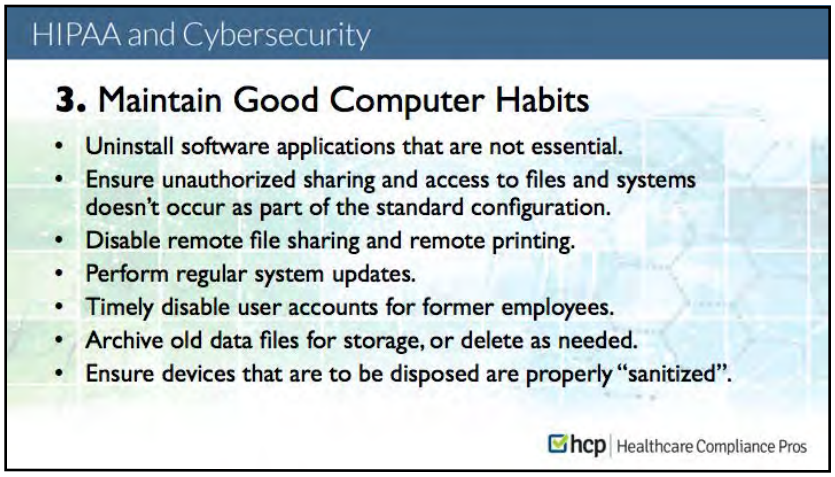
1. Establish a Security Culture

- A security-minded culture ensures good habits and practices become automatic.
- All employees should receive security training at the time of hire, whenever there are updates, and on an annual basis thereafter.
- All employees who access protected health information must understand your organization's policies and procedures.
- Leaders and managers in healthcare organizations need to set good examples.
- All employees should be encouraged to take responsibility for information security.
- The privacy and security of patient health information must be a priority.

SLIDE 16

2. Protect Mobile Devices

- Mobile devices that create, access, and store PHI are becoming more commonplace. As a result, we need to pay special attention to how we are safeguarding these devices.
- Ensure your mobile devices are equipped with strong authentication and access controls. For example, require unique user IDs and strong passwords (more on that later).
- Do not transmit unencrypted PHI across public networks. For example, do not send an email containing PHI while using Starbuck's Wi-Fi.
- Do not use mobile devices that cannot support encryption.
- Develop and implement policies and procedures that specify circumstances under which devices may be removed from the facility.
- Prevent unauthorized viewing of PHI displayed on a mobile device through training and domain policies.



SLIDE 17

3. Maintain Good Computer Habits

- Uninstall software applications that are not essential to running the practice. For example, games, photo sharing tools, etc.
- Instead of accepting defaults or "standard" configurations when installing software to ensure unauthorized sharing and access to files and systems does not occur as part of the standard configuration.
- Disable remote file sharing and remote printing within the operating system.
- Perform regular system updates, preferably these updates are automated.
- Disable user accounts for former employees at the time of separation. If the employee is being involuntarily terminated, remove access to the account prior to the notice of termination is given.
- Archive old data files for storage if needed, or clean them off the system if not needed.
- Ensure devices that are to be disposed are properly "sanitized" especially if these devices have had data stored on them.

SLIDE 18

4. Use a Firewall

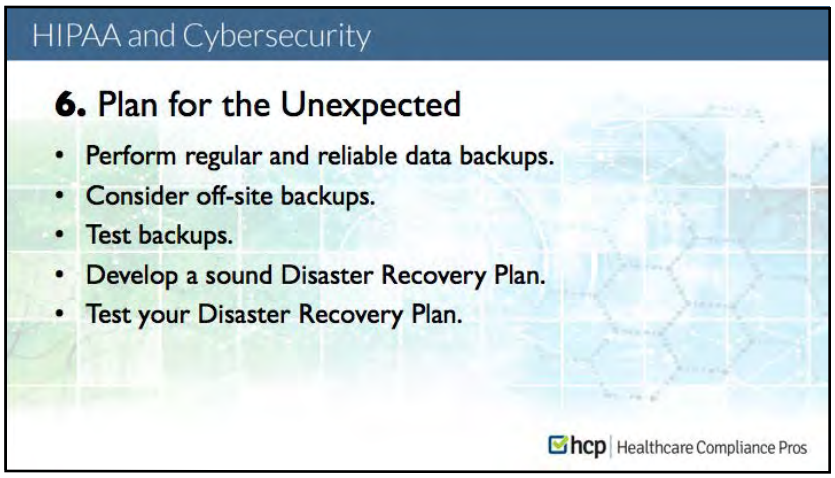
- Install a firewall to protect against intrusions for outside sources.
- Large practices that use a Local Area Network (LAN) should consider a hardware firewall. This will provide central management of firewall settings.
- Generally, a specialist will configure, monitor and maintain a hardware firewall.

Locate a professional with experience properly configuring firewall settings. A poorly configured firewall may give the practice a false sense of security.

SLIDE 19

5. Install and Maintain Anti-Virus Software

- Install and use an anti-virus product that provides updated on a regular basis for protection against viruses, malware and other malicious code that can attack your computers through downloads, email, etc.
- Keep anti-virus software up to date with the latest updates.



SLIDE 20

6. Plan for the Unexpected

- Perform regular and reliable data backups. We highly recommend encrypting all backups.
- Consider off-site backups, or cloud storage.
- Test backups. Don't assume the data is reliable every time.
- Have a sound Disaster Recovery Plan and keep it updated.
- Test your Disaster Recovery Plan. Keep a copy on-site and at least on copy off-site.

SLIDE 21

7. Control Access to Protected Health Information

- Your EHR should be configured to grant PHI access to those with only a need to know.
- Manually set these permissions (e.g. identify which files should be accessible to which staff members).
- Configure role-based access control as needed.

Real world example of access control

Recently, during a HIPAA Walkthrough and Security Risk Analysis, we discovered a practice who decided for workflow purposes, that they would use logins based of clinic location rather than requiring unique usernames and passwords for individuals. In doing so, they allowed access by anyone who works in that area of the clinic to parts of the EHR that only those with a need to know (i.e. physicians) should be accessing.

SLIDE 22

8. Use Strong Passwords and Change Them Regularly

- Your password should not be easy to guess.
- Do not use your date of birth, names, etc.
- Do not reuse passwords and if so, rotate them.
- Do not share your passwords with other users.

We recommend the following:

A password that is at-least eight characters in length

A password that is multi-case requiring at least one upper case letter, one lower case letter, a number and one special character.

Require passwords to be changed periodically – no longer than six months. Preferably, passwords should be changed every 90 days or less.

SLIDE 23

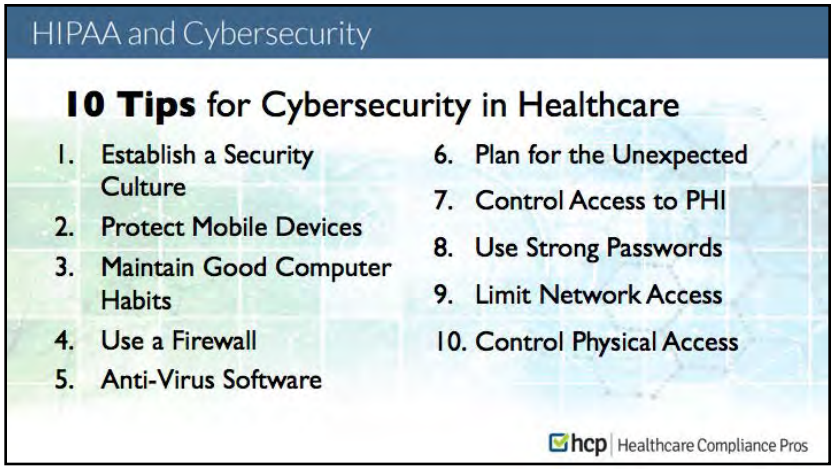
9. Limit Network Access

- Prohibit staff from installing software and/or hardware without prior approval.
- If you are using a wireless router ensure it is set up to operate only in encrypted mode.
- Prohibit casual network access by visitors. For example, if you allow guests to access internet, have a separate network that cannot access ePHI.
- Ensure file sharing, instant messaging, and other peer-to-peer applications have not been installed – unless you have determined they are allowed based on a risk analysis. Then, these applications should only be installed if approved.

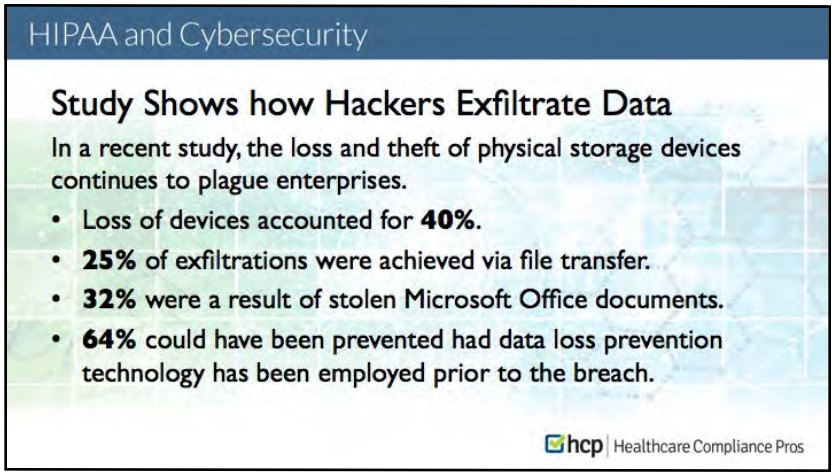
SLIDE 24

10. Control Physical Access

- Limit and to the best of your ability prevent chances that devices may be tampered with, lost or stolen. For example, if you are transporting a laptop that has access to PHI, or has stored PHI on drives, do not leave the laptop unattended in a car or other unsecure locations.
- Document and enforce policies limiting physical access to devices, information, and the facility.
- Monitor and control access to hard copy PHI. Locks, pin pads, and key cards all provide access control measures.



SLIDE 25



SLIDE 26

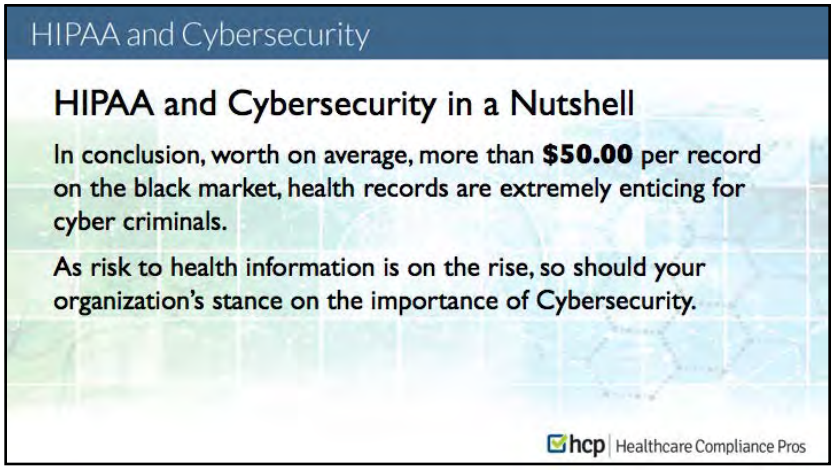
Study Shows how Hackers Exfiltrate Data

- In a recent study, the loss and theft of physical storage devices continues to plague enterprises.
- Loss of storage devices, laptop computers and tablets accounted for 40 percent of data exfiltrations.
- For 25 percent of cases, data exfiltration was achieved via file transfer or tunneling protocols.
- 32 percent of all stolen data were a result of stolen Microsoft Office documents.
- In 64 percent of cases, IT professionals quizzed in the study believe that data loss could have been prevented had data loss prevention technology has been employed prior to the breach.

SLIDE 27

Is Data Stored in the Cloud more susceptible to an attack?

- The short answer to this is no – as long as technologies to secure cloud based applications are implemented.
- According to McAfee's "Grand Theft Data" study, while there are some security vulnerabilities that do exist, overall the cloud appears to be secure. In fact, according to the study, cloud applications pose no greater risk than internal storage systems. This obviously is dependent on what technologies have been implemented to secure their cloud based applications.



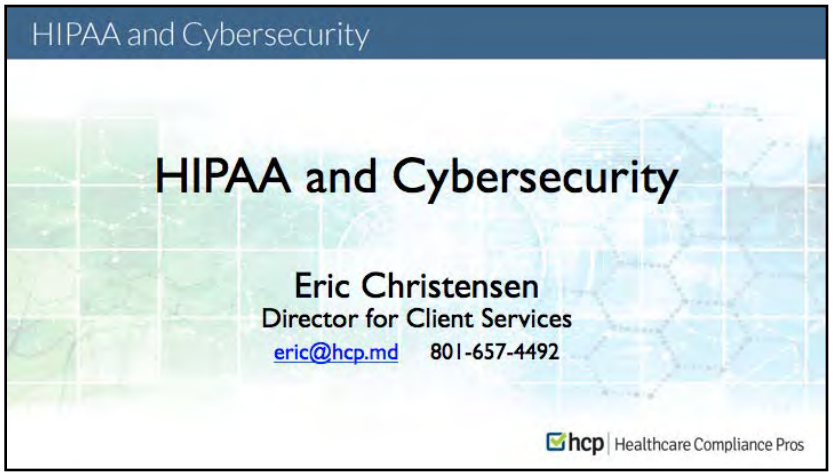
SLIDE 28

HIPAA and Cybersecurity in a Nutshell

In conclusion, worth on average $50.00 per record on the black market, health records are extremely enticing for cyber criminals.

As risk to health information is on the rise, so should your organization's stance on the importance of Cybersecurity. Rather than being our own worst enemies, we can proactively protect patients' health information and protect all of our systems that create access and store this information – physical, electronic, mobile devices and cloud – before attacks or theft occurs.

SLIDE 29



SLIDE 30