PACAH Spring Conference – April 19, 2022

Identifying and Mitigating Cybersecurity Threats

Cynthia A. Haines, Post & Schell, P.C

Post & Schell P.C.
ATTORNEYS AT LAW

Health Care Facilities and Cyber Crime

- Health care facilities are increasingly the targets of cyber criminals.
  - Nursing homes and other long-term care facilities do not always have dedicated IT professionals.
  - Despite that, they still need to adopt security practices and technical solutions needed to defend sensitive data against intentional and unintentional threats.

Objectives

- Learn how to recognize, prevent and mitigate threats, including loss or theft of equipment, ransomware attacks, hacking and email phishing.
- Determine when incidents and breaches may be reportable under federal and state requirements.
- Understand crucial risk management for cyberthreats:
  - Staff training
  - Computer security practices
  - Hardware and software solutions
  - Cyber insurance

What is a Cybersecurity Threat?

- **External threats**: Threats made by outside organizations or individuals, attempting to get into your network.
- **Internal threats**: These are threats from malicious insiders, such as disgruntled or improperly vetted employees.
- **Structured threats**: Organized attacks by attackers who know what they're doing and have a clear aim or goal in mind. Government-sponsored attacks, for example, fall into this category.
- **Unstructured attacks**: Disorganized attacks, often by amateurs with no concrete goal in mind.

Threat vs. Vulnerability

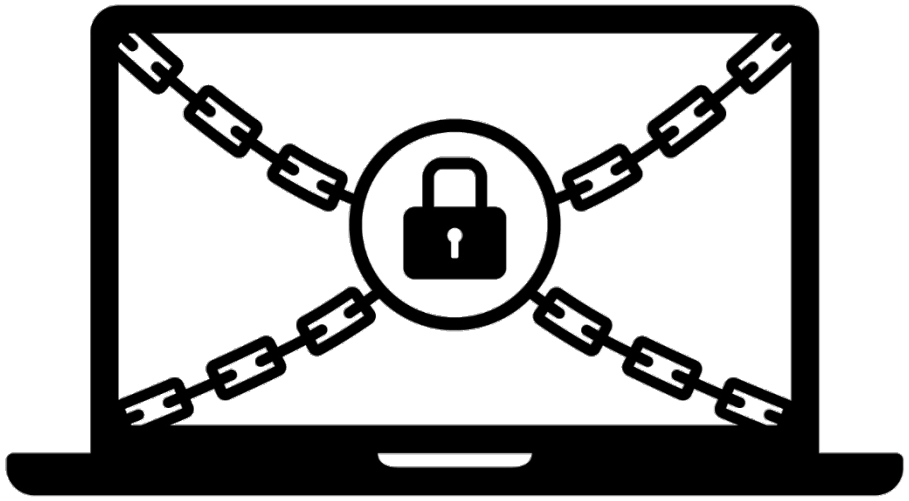
- Vulnerabilities are flaws in your systems that can be exploited by attackers. These are often not malicious errors, but simply mistakes or things that have been overlooked.
- It's not just clouds and software – vulnerabilities can be people as well.
- If you haven't trained your employees about avoiding clicking on suspicious links, for example, they can be vulnerable to phishing.

Network Threats-Phishing

- Phishing attacks are attempts to trick people into opening suspicious links or downloading malicious programs.
- They range from the easily-spotted to sophisticated cons targeting a specific individual.
- Phishing campaigns are currently one of the most popular methods of attack, according to Microsoft.

Network Threats-Ransomware

- Often delivered via successful phishing campaigns, ransomware enters your systems, encrypts your data, and holds it hostage until you pay the attackers' ransom. Once the ransom is paid, the attackers will allegedly give you control of your data, but criminals don't always keep their word.



Network Threats-Ransomware

- Erie County Medical Center (ECMC) in April 2017. The ransomware attack took down 6,000 ECMC computers over the course of six weeks.
- Even though the cyberattack was discovered within hours, all computer systems were locked down, driving providers back to pen and paper.
- For two weeks, ECMC staff worked without email access and had to manually register patients. It took three weeks for lab results and other communications to be electronically delivered.
- It took months for the system to recover and cost nearly $10 million to recover from the attack.

Network Threats – Malware

- Any malicious program that enters your system, malware can be ransomware, a virus, or a worm that infects first a device, then the whole network.

Network Threats-Malware

Malware encompasses all types of malicious software, including viruses, and cybercriminals use it for many reasons, such as:

- Tricking a victim into providing personal data for identity theft
- Stealing consumer credit card data or other financial data
- Assuming control of multiple computers to launch denial-of-service attacks against other networks
- Infecting computers and using them to mine bitcoin or other cryptocurrencies

Network Threats-DDoS, APT, SQL Attacks

- **DDoS (Distributed Denial attacks):** DDoS attacks overwhelm your servers with requests for information, forcing sites, servers, and applications to shut down.
- **APT (Advanced Persistent Threats):** During an APT attack, an unauthorized attacker codes into a system network and stays there quietly, collecting information.
- **SQL (structured query language) Injection:** SQL injection attacks inject malicious code into a site or application using SQL queries in order to exploit security vulnerabilities and obtain or destroy private data.

Identifying Threats and Vulnerabilities

- **Watch your own network:** The most important way to identify threats and vulnerabilities is to make sure you can see them. You want to be able to look at your defenses the way an attacker would, understanding the weaknesses in your network and the threats most likely to affect your organization.
    1. Determine which threats to prioritize
    2. Choosing continuous monitoring tools
    3. Train employees on cybersecurity best practices

Learn about Threats

- What sort of attacks are being launched, and which threats might your organization attract?
- By understanding the current threats, you can protect your organization against threats before they happen.
- Work proactively, rather than reactively.
- Applying insights obtained via threat data allows security teams to make quicker, more informed security decisions so they can stay one step ahead of cyber threats.

Identifying Threats

- **Penetration testing**: Which employee is likely to click a bad link in a suspicious email. You can't know until you test your defenses, and penetration testing is the best way to do that.
- **Manage permissions**: By segmenting your network and managing permissions so that not every employee can access every part of your network, you can control who sees what — and also protect your network against data breaches and malicious insiders.
- **Use a firewall**: there's no reason not to use firewalls, internally and externally. Firewalls keep unauthorized users from getting access to your network. They also keep tabs on the traffic throughout your network.

Breaches – Overview

- The Health Insurance Portability and Accountability Act (HIPAA)
  - The Legal Framework of HIPAA
  - Training, Managing and Tracking Access to PHI
- Risks of a Data Breach
  - Possible Penalties
  - Reputational Harms
- HIPAA Breach Assessment and Response
  - Types of Breaches
  - Breach Response
- Other Laws

The Legal Framework

- The Health Insurance Portability and Accountability Act (HIPAA)
- Public Law 104-191 (1996)
- Overseen by: Department of Health & Human Services ("HHS") and enforced by Office for Civil Rights ("OCR")
- Regulations on:
  - Privacy of health information
  - Security of health information
  - Notification of breaches of confidentiality
  - Penalties for violating HIPAA

Risks of a Data Breach

- Civil Monetary Penalties (CMPs) based on tiered civil penalty structure depending on the level of culpability as determined by the Secretary of HHS
  - Unknowing - $100 to $50,000 per violation
  - Reasonable cause - $1,000 to $50,000 per violation
  - Willful neglect corrected within 30 days - $10,000 to $50,000 per violation
  - Willful neglect not corrected within 30 days – no less than $50,000 per violation

Risks of a Data Breach

- OCR can refer HIPAA violations to the Department of Justice (DOJ)
  - Directors, officers or employees could be deemed criminally liable
  - Different levels of severity depending on the level of culpability
    - Penalties range from a fine of $50,000 and imprisonment up to one year to a fine of $250,000 and imprisonment up to 10 years
    - Restitution possible if residents/patients have been defrauded

Risks of a Data Breach

- Reputational Harm
  - OCR maintains a *permanent* and *searchable* breach portal (aka the "Wall of Shame") listing breaches of unsecured PHI affecting 500 or more individuals
    - The Wall of Shame includes the details of the breach including the name of the entity breached, the type of breach, the location of the breach and the number of people affected
  - News Coverage

Enforcement Results As Of July 31, 2018

- **To date:** 186,453 HIPAA complaints filed, and OCR has initiated over 905 compliance reviews
- OCR investigated and resolved over 26,152 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA CEs and their BAs
- OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the CE or their BA
- OCR has settled or imposed a civil money penalty in 55 cases resulting in a total dollar amount of $78,829,182.00
- In another 11,518 cases, OCR investigations found no violation had occurred

HIPAA Breach Assessment and Response

- What is a Breach?
  - A Breach is an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational or other harm to the individual

Types of Breaches

- Hacking/IT Incident
- Unauthorized Access/Disclosure
- Theft
- Improper Disposal
- Loss
- Other

How Breaches Can Occur: Examples

- Faxing PHI to the wrong fax number
- Theft or misplacement of a laptop, tablet, flash drive, or CD containing PHI
- Clicking on a link in an email or using a computer infected with a virus or malware
- Improperly disposing of electronic equipment containing PHI
- "Snooping" by members of the workforce

Breach Assessment and Response: Questions To Consider

- Was there a breach?
- Do individuals need to be notified?
- Why did this occur?
- How will the breach be mitigated?
- How do we prevent this from happening again?
- Who needs to be involved in risk analysis/ mitigation/future prevention?

Breach vs. Incident

- **Breach**
  - Acquisition, access, use or disclosure of PHI
  - In a manner not permitted under the HIPAA Privacy Rule
  - Which compromises the security and privacy of PHI
- **Incident**
  - The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system

Exceptions to Breach

- *Unintentional* access or use by workforce member if
  - Made in good faith
  - Within scope of authority to access
  - Does not result in further breach
- Inadvertent disclosure from one authorized person to another *authorized* person
- Disclosure where CE has good faith belief that person receiving the information would not reasonably be able to retain such information

Presumption of Breach

- Impermissible access, use or disclosure of PHI is ***presumed*** a breach ***unless*** Covered Entity ("CE") or Business Associate ("BA") shows a "low probability" that PHI has been "compromised"

- Determine such probability based on risk assessment

Risk Assessment Factor 1

- Nature/extent of PHI involved, types of identifiers and re-identification risk
  - Whether data is of a sensitive nature
  - Financial, credit card, SSN, DLN
  - Risk of ID theft?
  - Type, amount and effect of clinical data
  - Potential for harm to individual or value to unauthorized person

Risk Assessment Factor 2

- Unauthorized user or unauthorized recipient
  - Differences between snoopers, hackers and surfers
  - ID thief versus hardware thief
  - Does recipient have duty to protect?
  - Ability to re-identify

Risk Assessment Factor 3

- Was PHI *actually* accessed or used?
  - Must consider actual vs. opportunity
  - Must affirmatively show PHI not accessed
  - Cannot just assume no access
  - System/computer forensics used as example

Risk Assessment Factor 4

- Extent risk to PHI has been mitigated
  - Always attempt to mitigate - quickly
  - Consider obtaining assurances
    - Keep PHI confidential
    - Agree to return/destroy
  - Keep in mind HIPAA Security Rule requirements on responding to security incident, reassess risk, manage risks

Breach Response:
We Have a Breach, Now What?

- Notification
  - Upon discovery of a
  - Breach of
  - Unsecured PHI
  - A CE and a BA must notify
  - Individuals, HHS and sometimes media (>500)
  - Subject to certain exceptions

Notification to Individual

- Must be timely –
  - Without unreasonable delay
  - No later than 60 days
- Must be in writing
- Elements
  - Description of what happened
  - Date of breach
  - Date of discovery
  - Description of PHI involved
  - Steps the person should take to protect self
  - Steps CE is taking to investigate, mitigate and protect from future breaches
  - Contact information to ask follow up questions

Notification to Media

- Only if breach involves more than 500 residents of a state or jurisdiction
  - Notify prominent media outlets serving the state or jurisdiction
  - Same elements as notification to individual

Notification to Secretary of HHS

- If **more than 500** individuals involved
  - Must notify Secretary at the same time CE notifies individual
  - HHS website describes manner of notification
- If **less than 500** individuals involved
  - Maintain a log
  - Provide log to Secretary within 60 days following end of calendar year
  - HHS website describes manner of notification

Pennsylvania Data Breach Notification Law

- The Act's requirements extend to any business organization, whether for-profit or not-for-profit, and any state agency or local political subdivision, that "maintains, stores or manages computerized data that includes personal information."
- The notification requirements of the Act are triggered when there is a breach of the security of a computerized data system "to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person."

Pennsylvania Data Breach Notification Law

- "Personal information" is defined to mean an individual's "first name or first initial and last name in combination with and linked to" the individual's unencrypted or unredacted social security number, driver's license number or other state identification card number, or any financial account number, credit or debit card number in combination with any security code, access code or password that would permit access to the individual's financial account.
- Notice of a security breach must be made "without unreasonable delay."

FTC Health Breach Notification

- The Rule applies to:
- a vendor of personal health records (PHRs);
- a PHR related entity; or
- a third party service provider for a vendor of PHRs or a PHR related entity.

21st Century Cures Act

- Passed in 2016 after ONC "Report on Information Blocking" indicated that market and economic conditions were creating incentives for some persons and entities to unreasonably limit access to electronic health information.

- Calls for all electronically accessible health information to be accessed, exchanged, and used "without special effort on the part of the user."

21st Century Cures Act

- Prohibits "information blocking," defined as a practice that is "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information" and which . . .
  - If conducted by a provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.
  - If conducted by a Health IT developer, exchange, or network, such entity knows or should know that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.
- Information blocking does not include a practice that is required by law.

How Do APIs in Healthcare Work?

How Do APIs in Healthcare Work?

1. A patient downloads the health app of her choice.
2. The patient logs into the app and creates a username and password for the app.
3. The patient uses the app to link securely to an API for the health care provider.
4. The app sends a request to the provider asking for access to the patient's medical records.
5. The health care provider's server validates the request coming from its API, fulfills the criteria, and sends back the patient's data in a structured format.
6. The patient can now access health information from the app.
7. The patient repeats steps 3-6 with other health care providers that have granted access to the app.
8. Depending on the app, the patient can now merge the health information from multiple sources, to access all their health information in once place.

ONC Final Rule – Information Blocking

- Information Blocking: a practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI)
  - Includes a health care provider that knows such practice is unreasonable and is likely to do any of the above.
  - **"Interfere with":** to prevent, materially discourage, or otherwise inhibit,
- Applicable to "actors" (providers, developers of certified Health IT, and HIN/HIE).

ONC Final Rule – Information Blocking

- A practice is not information blocking if it is required by law or if it satisfies an enumerated exception:
  - Preventing Harm
  - Privacy
  - Security
  - Infeasibility
  - Health IT Performance
  - Content and Manner
  - Licensing
  - Fees are allowed-must be reasonable

Security Exception

- An actor may interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided:
  - The practice is directly related to safeguarding the confidentiality, integrity, and availability of electronic health information;
  - The practice is tailored to the specific risk being addressed;
  - The practice is implemented in a consistent and non-discriminatory manner; and
  - The actor is either following an organizational security policy that aligns with one or more consensus-based standard or best practice guidance, or makes a determination based on the particularized facts and circumstances.

Interoperability And Privacy/Security

- Interoperability regulations will require a new orientation for providers.
- For decades providers have been focused on protecting the privacy and security of EMR; now they will have to devote equal concern to ensuring access to EMR to facilitate the flow of electronic health information.
- E.g., information blocking rule may require providers to provide access to PHI in circumstances where HIPAA would not.
  - Generally, HIPAA permits, but does not require disclosure of PHI.
  - ONC Final Rule also requires providers to take affirmative steps (e.g., making reasonable efforts to provide authorization forms).

Interoperability And Privacy/Security

- ONC & CMS rules elevate use of third-party smartphone health apps.
- Apps are not subject to HIPAA.
- **ONC Final Rule**: Health care providers are permitted to provide factually accurate, objective, unbiased, non-discriminatory information about third-party apps to patients, but must avoid information blocking.
- **CMS Final Rule**: Payors are required to share educational resources with patients to help them be informed about the risks of sharing data with apps.
- **CMS Final Rule II**: Certain payors must require apps to attest to having certain privacy and security provisions in privacy policies.

Protections

- Vigilance
  - Review policies and procedures
  - Document implementation
  - Document training and attendance
  - Encryption
- Risk Analysis
  - Review HHS Risk assessment tool
- Top-down buy in
  - Board must be involved
- Cyber Insurance

Policy Content: Key Points

- People consider health information their most confidential information, and as such the we must protect it accordingly:
  - Do not access PHI that you do not need
  - Do not discuss PHI with individuals who do not need to know it
  - Do not provide PHI to anyone not authorized to receive it
  - Misusing PHI can result in discipline, legal penalties and loss of trust

Policy Content: Key Points

When using PHI, think about:

- Where you are
- Who might overhear
- Who might see

Avoid:

- Discussing PHI in front of others who do not need to know
- Leaving records accessible to patients or others who do need to see them
- Positioning monitors where others can view them
- Using printers located in public or unsecured areas

Policy Content: Key Points

Do not engage in risky practices with computers used to access PHI:

- Do not surf the internet
- Do not open attachments to e-mail unless from a trusted source
- Do not install applications unless approved by IT Department

Policy Content: Key Points

- Do not unnecessarily print or copy PHI
- When faxing PHI, use a fax cover page
- Do not send PHI in email unless first cleared by your supervisor
- Dispose of PHI when it is no longer needed
- Use shredding bins for paper records
- When retiring electronic media used to store PHI, ensure the media is "cleansed" according to IT Department standards
- Call Help Desk for more details

Policy Content: Key Points

- Report unusual activity to your supervisor immediately
- You observe questionable practices
- You find PHI in inappropriate areas
- You suspect unauthorized use of your user ID/password

Policy Content: Key Points

- The consequences of failing to adhere to the policy
  - CEs must have and apply appropriate sanctions against those who violate policies and procedures in order to deter noncompliance
  - Should be aimed at reinforcing the substance of the HIPAA access policy

Staff Training

- Employees who are cyber aware are more likely to regularly update their systems and applications, bolstering your organization's overall cybersecurity.
  - Depending on their level of expertise, employees can also help identify potential vulnerabilities within systems.
- For this reason, it is recommended that you create a program for employee cybersecurity education.
  - Unfortunately, no continuous security monitoring program can be guaranteed as one-hundred percent effective, but with a cyber aware workforce, you can make sure low-level threats are properly addressed.

Training

- Both the Privacy Rule and the Security Rule impose training requirements
  - In general, anyone who comes into contact with PHI must be trained
- Neither Rule specifies the exact content of the required training
  - In general, training should be keyed to each person's role in the organization

Training, Managing and Tracking Access to PHI

- The Security Rule specifies safeguards that CEs must implement to protect ePHI confidentiality, integrity and availability. Specifically, CEs must:
  - Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated impermissible uses or disclosures; and
  - Ensure compliance by their workforce

Training, Managing and Tracking Access to PHI

- Covered entities (CEs) are required to have policies and procedures in place regarding the handling of PHI
  - These security measures should be designed to reduce risks and vulnerabilities
    - This is not one-size-fits-all
  - CEs must designate a security official who is responsible for developing and implementing its security policies and procedures

Best Practices When On- and Off-Boarding Employees

- Designate a department or individual to monitor and approve access and use of systems containing PHI/ePHI
- Have a system in place to track which employees have access to which systems and physical locations
- Control access and rights to all devices issued to employees
- Require all new employees to have their own individual logins and passwords
- Don’t let employees have administrative rights to computers

Off-Boarding Policies and Protocols

- Designate someone to be the point-person who "owns" off-boarding
  - Use a checklist so nothing is forgotten or overlooked
  - Take actions to remove access as quickly as possible
  - Notify and coordinate with IT and/or security when employees leave/give notice

Key Points for Off-Boarding

- Terminate electronic access to PHI
  - Remove departing employee from authorized user lists, email distribution lists
  - Change passwords for remote computer systems (VPN, remote desktop, and remote web tools)
  - Change passwords and PINs for on-site workstation, voicemail and email
  - Terminate electronic accounts if necessary
  - Collect mobile devices and other company-owned physical assets and files
  - Purge any PHI that may be on departing employee's personal devices and terminate access to PHI from such devices going forward.

Key Points for Off-Boarding

- Terminate physical access to PHI
  - Turn off keycard access
  - Collect physical keys, keycards, ID badges, and security tokens
  - Change combination locks, PINS and security codes

Enforcement and Logistics

- Timing/Urgency
  - Circumstances matter!
    - Mobile device management solutions
- Distribution list for departures
  - Inform key departments when employees leave
- Discipline task owners who do not follow off-boarding protocols
  - The role of audits

Computer Security Practices

- Ongoing maintenance, upgrades and performance monitoring.
- Internal controls and processes for software and upgrades.
- Investigation and collaboration in response to technology-related deaths, serious injuries, unsafe conditions, complaints and regulatory investigations.
- Transparency about issues.
- Training and education of users.
- Strong Contracts

Computer Security Practices

Third party data storage:

- A medical professional or a healthcare organization creating ePHI that is stored by a third party, is required to have a Business Associate Agreement (BAA) with the party storing the data.
- The BAA must include methods used by the third party to ensure the protection of the data and provisions for regular auditing of the data's security.

Computer Security Practices-Safety

- Ongoing maintenance, upgrades and performance monitoring.
- Internal controls and processes for software and upgrades.
- Investigation and collaboration in response to technology-related deaths, serious injuries, unsafe conditions, complaints and regulatory investigations.
- Transparency about issues.
- Training and education of users.

Interoperability and Integration

- Compatibility with the EHR.
- For example, a telehealth contract should not unduly restrict a provider's ability to integrate third party technologies and services that are important to the provider's ability to leverage data to deliver better and more efficient care, or to take advantage of emerging technologies.
- Interface strategy – point-to-point, data feed or batch export capabilities.
- Ability to integrate third party products.

Security

- Security assessment.
- Independent security audit.
- Provider's information security program and industry standards (e.g., NIST) as the baselines.
- Encryption methodology and secure data retention and destruction.
- Compliance with applicable state and federal data security regulations.

System Performance

- Contract should describe all core service and performance obligations:
  - Acceptance criteria for equipment and software,
  - Uptime and system response time,
  - Quality and timeliness of service,
  - Post implementation support,
  - Performance management strategies – e.g., SLAs for unscheduled system downtime.

Data Rights

- Contract needs to specify that:
  - The provider owns all telehealth data and has timely and reliable access to it.
  - The provider may access data for maximum analytical value.
  - Acknowledge the importance of data in patient care.
  - Restrict the scope of vendor's use and commercialization of data.
  - Vendor must adequately respond to emergencies.
  - System will facilitate patient access.

Computer Security Practices – IT Investment

- Investment in IT will be necessary to meet deadlines and ensure that the educational and privacy elements of the new regulations are met.
  - It will be important to:
    - Standardize data collection and reporting which produces quality data imperative for successful interoperability.
    - Update HIPAA policies (HIPAA permissible disclosures are now required unless an exception applies).
    - Conduct a Security Risk Assessment.
    - Be proactive with EHI requests.
    - Review fees associated with EHI requests.
    - Revise Business Agreements and Notices of Privacy Practices.
- Be sure that all EHI is remaining secure and being transmitted through secure channels.

Computer and Security Practices

- EHR should not unduly restrict a provider's ability to integrate third party technologies and services that are important to the provider's ability to leverage data to deliver better and more efficient care, or to take advantage of emerging technologies.
- Interface strategy – point-to-point, data feed or batch export capabilities.
- Ability to integrate third party products.
- Strong Contracts.

Best Practices – Information Blocking

Re-evaluate contracts, privacy practices, and other policies and procedures to ensure that they are not unreasonably interfering with a patient's access or use of EHI.

- This may include analyzing:
  - How requests for EHI from health care providers and others are handled.
  - Whether current data privacy and security policies comply with new information blocking prohibitions.
  - Whether fees charged in relation to access, exchange, or use of EHI satisfy the conditions of the "Fees Exception."
  - How existing EHR vendor contracts, data-use agreements and other information sharing arrangements function.

Best Practices – Information Blocking

- Be aware that EHR vendors that are certified Health IT developers are also subject to the rule.
- Health care providers are not required to agree with contractual terms that enable EHR vendors to engage in information blocking.
- Insist on terms that enable and encourage interoperability and clearly prohibit vendor blocking.

Best Practices – Interoperability Strategy

- Health care providers need to determine their interoperability strategy.
  - Seek input from all affected stakeholders to avoid potential criticism and more formal challenges in the future.
- Consider how to measure success.
  - Identify key performance indicators.
- Remember that interoperability is an investment in the future and an opportunity to be leaders in the provider market.

Best Practices-Cyber Insurance

- Ransomware and other cyberattacks on the health care industry have been on the upswing.
- Insurers require providers need to meet certain standards and minimum requirements facilitates HIPAA compliancy and therefore mitigate the risks of hefty HIPAA fines for non-compliance
- According to a 2021 IBM Data Breach Report, the average cost of a health care data breach is now $9.42 million dollars.
- Cost for cyber insurance has become increasingly expensive. In a recent GAO survey of insurance brokers, more than half of respondents' clients saw prices go up 10% to 30% in late 2021.

Best Practices-Cyber Insurance

- A cyber insurance policy will cover losses and damages incurred by a breach or security event that includes the loss, exposure, improperly shared, or theft of patient data.
- Some coverage will also handle ransomware attacks, but health providers must ensure that the correct language is added to coverage when negotiating with an insurance agent.
- However, unlike with traditional insurance policies, there's no standard format for underwriting these types of policies. Purchasers need to research the differences in carriers, such as amounts and requirements of the holder.

Best Practices-Cyber Insurance

- Cyber insurance policy will include breach management and activity monitoring funds.
- May also choose to purchase coverage that includes the cost to repair or replace tools or systems that were damaged by a cyberattack.
- Cyber insurance may also cover the costs of investigations following the breach, along with the cost to notify residents and the public.

Resources

- **Federal Register 45 C.F.R. Part 160 and Subparts A and E of Part 164.**
- **Office for Civil Rights ("OCR") Website:** http://www.hhs.gov/ocr/office/index.html
- **OCR FAQ:** http://www.hhs.gov/ocr/office/faq/index.html
- **HIPAA List Serve:** http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html
- **Audit Program Protocol:** http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit /protocol.html

Resources

- **OCR Breach Notification website:** http://ocrnotifications.hhs.gov/
- **Medicare Learning Network, "HIPAA Privacy and Security Basics for Providers,"** *available at* http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf.
- **OCR Security Risk Assessment Audit Tool:** http://www.healthit.gov/providers-professionals/security-risk-assessment

Resources

- **Health Information Privacy Training Resources:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
- **Security Rule Guidance Materials:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
- **Technical Assistance from OCR Regional Offices:** http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html
- **Cost of a Data Breach 2021** https://www.ibm.com/downloads/cas/OJDVQGRY

Questions

Cynthia A. Haines

Principal and Co-Chair
Information Privacy & Security Practice Group
Post & Schell, P.C.
717.612.6051 (O)
chaines@postschell.com