Advanced Institute for
Anesthesia Billing &
Practice Management

Royal Sonesta Chase Park — St. Louis
September 15-18, 2024
aiabpm.com

Change Healthcare Cyber Attack and Ransomware/Anatomy of a Breach Response

September 15, 2024
9:00 a.m.

Arne Pedersen, MBA, FACMPE
Stacy Harper, JD, MHSA, CPC Partner

921 Sherwood Dr| Lake Bluff, IL 60044
O: 815.516.8808 C: 317.502.7350
6201 College Boulevard, Suite 500| Overland Park, KS 66211
O 913.327.5120 C 913.317.6045

Advanced Institute for
Anesthesia Billing &
Practice Management

Agenda

- Federal Law on Security
  - HIPAA – Security
  - PPACA – Section 1104
- February 21, 2024
- Impact to the Healthcare Industry
- Strategies going forward

Advanced Institute for
Anesthesia Billing &
Practice Management

Federal Law on Cyber Security

Key Take Aways

1. Establish and enforce an electronic security standard
2. Reduce the administrative burden
3. Seamless processing

Advanced Institute for
Anesthesia Billing &
Practice Management

HIPAA – Security

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to **develop regulations protecting the privacy and security of certain health information**.
- The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) **establish a national set of security standards** for protecting certain health information that is held or transferred in electronic form.
- The Security Rule **operationalizes the protections** contained in the Privacy Rule by addressing the **technical and non-technical safeguards** that organizations called "**covered entities**" must put in place to secure individuals' "electronic protected health information" (**e-PHI**).
- Within HHS, **the Office for Civil Rights** (OCR) has responsibility for **enforcing the Privacy and Security Rules** with voluntary compliance activities and civil money penalties.

Advanced Institute for Anesthesia Billing & Practice Management

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HIPAA – Security

- Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry.
- At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems for administrative and clinical functions.
- Today, the medical workforce is more mobile and efficient. The rise in the adoption rate of new technologies increases the potential security risks.

Advanced Institute for Anesthesia Billing & Practice Management

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HIPAA - Security

- A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.
- The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

Advanced Institute for Anesthesia Billing & Practice Management

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HIPAA - Security

- The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates.
- The HITECH Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule. HHS developed regulations to implement and clarify these changes.

Advanced Institute for Anesthesia Billing & Practice Management

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

PPACA - Sec. 1104. Administrative simplification

- PURPOSE OF ADMINISTRATIVE SIMPLIFICATION.—Section 261 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d note) is amended—
- (1) by inserting "**uniform**" before "**standards**"; and
- (2) by inserting "**and to reduce the clerical burden on patients, health care providers, and health plans**" before the period at the end.

https://www.congress.gov/111/plaws/publ148/PLAW-111publ148.pdf

Advanced Institute for Anesthesia Billing & Practice Management

PPACA - Sec. 1104. Administrative simplification

- Section 1104, Administrative Simplification, clearly states that Electronic Funds Transfers, or EFTs, need to be in place.
- According to subsection (B) ADOPTION REQUIREMENTS; EFFECTIVE DATES., CMS was required to develop a set of operating rules for EFTs and ERAs **no later than January 1, 2011**, and have them **effective no later than January 1, 2013**.
- In accordance with Section 1104, the language clearly states that **the purpose** of going electronic with payments and remittance advice was to **simplify and reduce paperwork**, which was to have **a positive net effect on the administrative burdens** of healthcare providers.
- It **does not state** whether a private entity can become a middleman and **charge fees**.

https://www.congress.gov/111/plaws/publ148/PLAW-111publ148.pdf

Advanced Institute for Anesthesia Billing & Practice Management

PPACA - Sec. 1104. Administrative simplification

- Payment processors often boost insurers' revenues by sharing the fees from virtual credit cards.
- One processor, VPay, says in its marketing materials that insurers can "make money on every virtual card transaction."
- In response to questions from ProPublica, **UnitedHealth**, which owns **Change Healthcare** and **VPay**, asserted that its services help medical clinics streamline recordkeeping, reduce administrative burdens, and accelerate payments.

https://www.propublica.org/article/the-hidden-fee-costing-doctors-millions-every-year

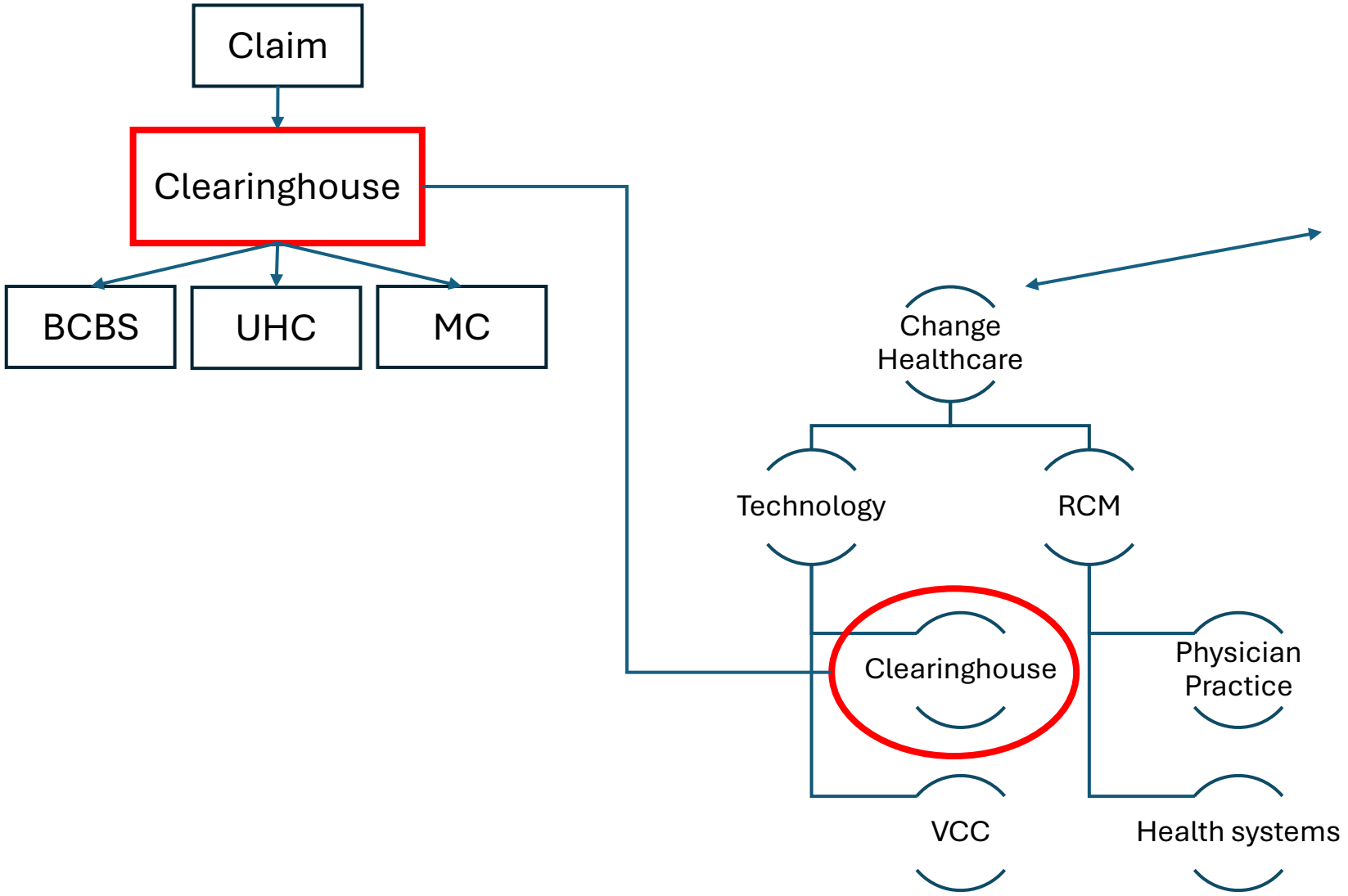
Advanced Institute for Anesthesia Billing & Practice Management

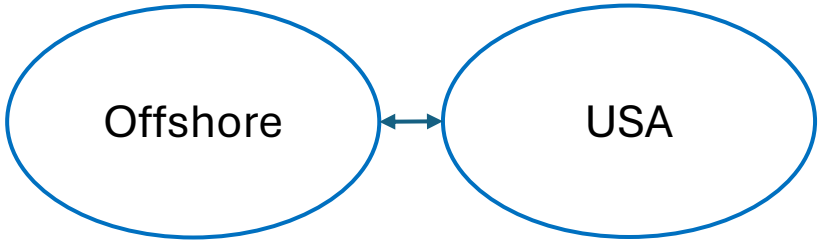
Key Take Aways

1. Establish and enforce an electronic security standard
2. Reduce the administrative burden
3. Seamless processing

Advanced Institute for
Anesthesia Billing &
Practice Management

Company Structure



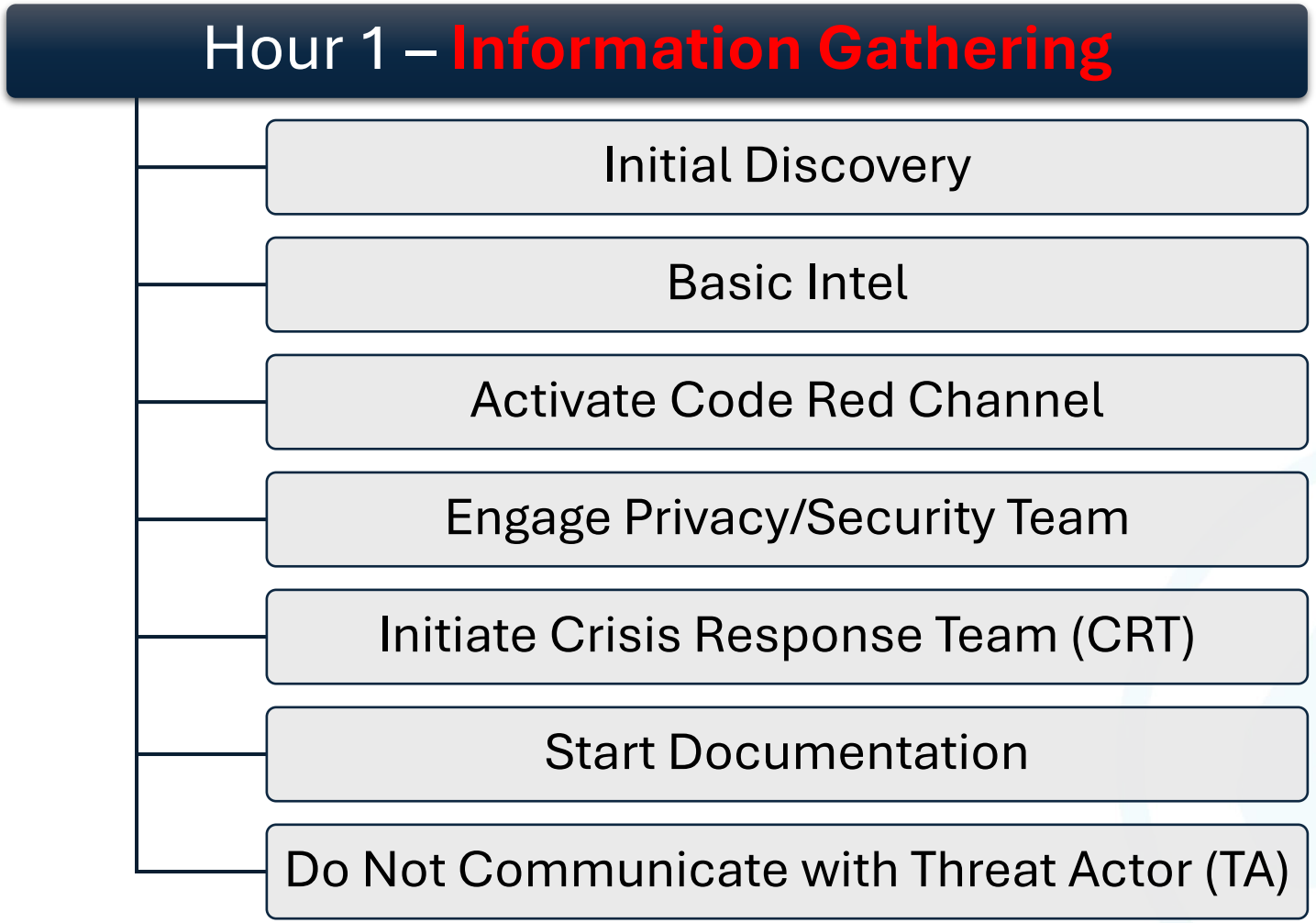


Advanced Institute for Anesthesia Billing & Practice Management

Breach Response

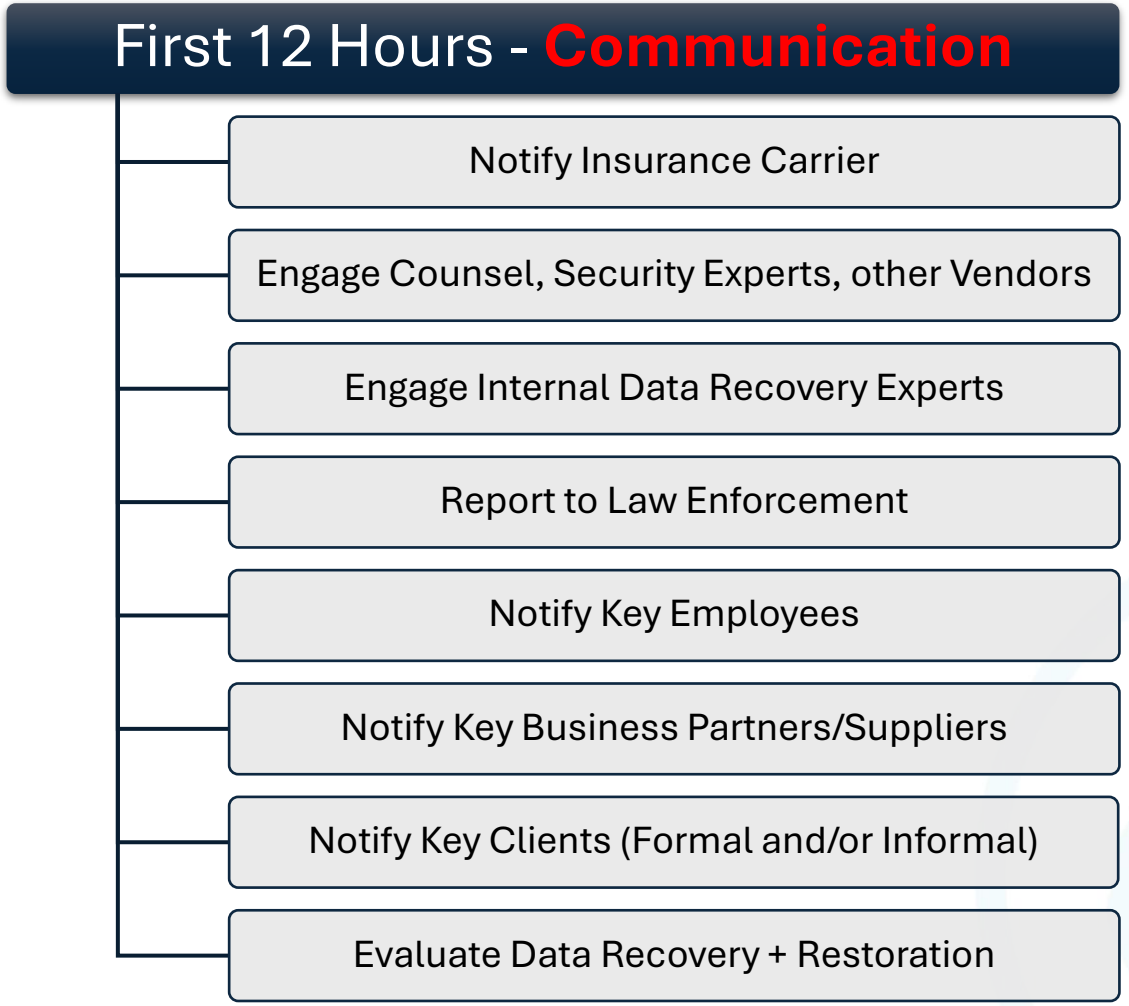
Hour 1 through first 72 hours

Ransomware Timeline



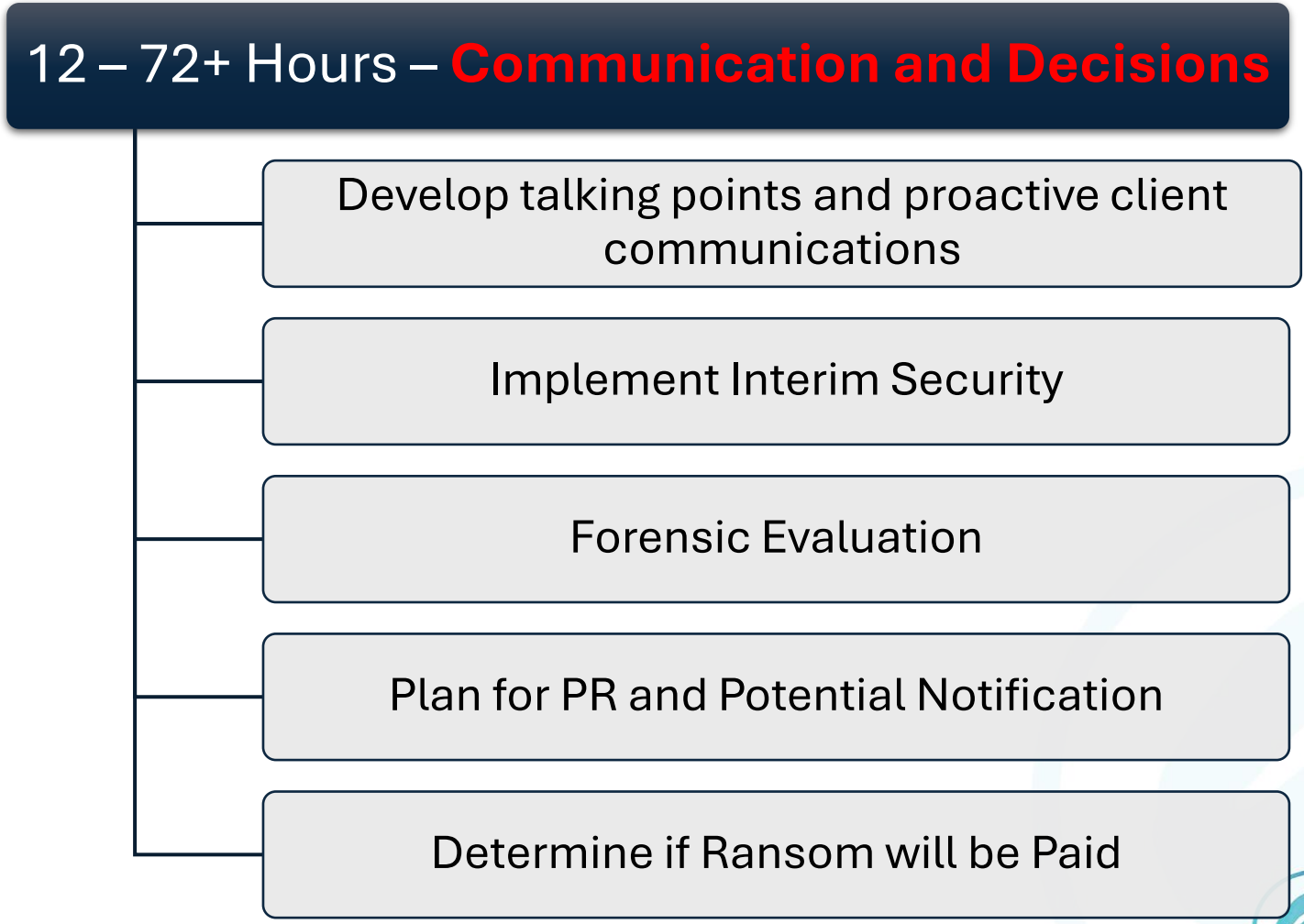
Advanced Institute for Anesthesia Billing & Practice Management

Ransomware Timeline



Advanced Institute for Anesthesia Billing & Practice Management

Ransomware Timeline



Advanced Institute for Anesthesia Billing & Practice Management

Ransomware Timeline

+ 8 Hours -72 + Hours – **Big Decisions and Communication**

If Ransom is Not Going to be Paid	**If Ransom is Going to be Paid**
Negotiate with Threat Actor	Negotiate with Threat Actor
Test Back-Ups and Recovery	OFAC Clearance
Begin Restoration Process	Carrier Approval for Payment
Obtain Evaluation from Forensics	Confirm Proof of Life
	Payment Transaction
	Obtain & Test Decryptor
	Begin Data Decryption Process
	Follow-up with TA if Problems
	Obtain Interim Signals from Forensics

Advanced Institute for Anesthesia Billing & Practice Management

Wednesday, February 21, 2024

CYBER ATTACK

On February 21, 2024, Change Healthcare—a healthcare technology company owned by UnitedHealth Group—issued a statement that it had been impacted by a ransomware attack. According to Change Healthcare, a “threat actor” gained access to its system. As a result of this cyberattack, Change Healthcare’s services have been shut down.

https://foleyhoag.com/news-and-insights/publications/alerts-and-updates/2024/march/change-healthcare-cyberattack

Advanced Institute for Anesthesia Billing & Practice Management

UnitedHealth CEO: Hackers used stolen credentials to access Change systems

- Mr. Witty submitted the written testimony prior to a House subcommittee hearing on May 1 regarding the Change ransomware attack. In his testimony, Mr. Witty said hacking group ALPHV, also known as BlackCat, "**used compromised credentials to remotely access a Change Healthcare Citrix portal**." This occurred Feb. 12, according to Mr. Witty.
- "**The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data**," Mr. Witty wrote. "**Ransomware was deployed nine days later**."

Advanced Institute for Anesthesia Billing & Practice Management

https://www.beckershospitalreview.com/cybersecurity/unitedhealth-ceo-hackers-used-stolen-credentials-to-access-change-systems.html

Change Healthcare Actions

- Immediately shut down systems
- Not all systems are up as of yet
- Provided loans to RCM clients: physician practices and Facilities
- Paid one ransom already of $22MM
- A second group claimed to have contract and patient data looking for another ransom
- CEO was called to Washington DC and sent a statement instead.

TIMELINE

- February 21, 2024 – Change Healthcare announces cyber attack
- All servers were taken off-line including the Clearinghouse and RCM business units
- Health systems, Hospitals, Physician Groups, and RCM companies using Change's clearinghouse and RCM are impacted
- Change Healthcare is shut down for 30 days
- The cyber criminals did get their ransom
- The cyber criminals have also begun to expose ePHI on the dark web
- United Healthcare Group CEO summoned to Washington DC by Congress and the White House

Impact to the Healthcare Industry

Impact

- The single-largest cyber security attack in the US Healthcare industry.
- It is has been dubbed the “Colonial Pipeline” for healthcare.
- As shared with the public, Change Healthcare shut down all of their systems. Their clearinghouse was rendered inoperable due to the cyber attack.
  - **No claims submissions**
  - **No claims payments**
  - **No notices**
  - **NOTHING for over 30 days**

Advanced Institute for Anesthesia Billing & Practice Management

Impact

- Physician practices
  - 30-day stoppage of cashflow
  - Most practices do not have a 90-to-120-day cash reserve
  - Scrambled to find different ways to submit claims and get payment
- Hospitals and Health Systems
  - 30-day stoppage of cashflow
  - Most do have a 120-day cash reserve
  - Scrambled to find different ways to submit claims and get payment
- Revenue Cycle Management Companies
  - For those who sole sourced claims submission and payments through the Change Healthcare clearinghouse, dead in the water.
  - Scramble to find different ways to submit claims and get payment

Impact

- Change Healthcare processes about 15 billion healthcare transactions annually, handling 1 in 3 patient records.
- Claims are flowing for both submissions and payments but not at the previous pace
- Millions of Americans ePHI is being exposed. Americans must be ready for the largest cyber attack American civilians ever. The elderly are the most vulnerable

Advanced Institute for Anesthesia Billing & Practice Management

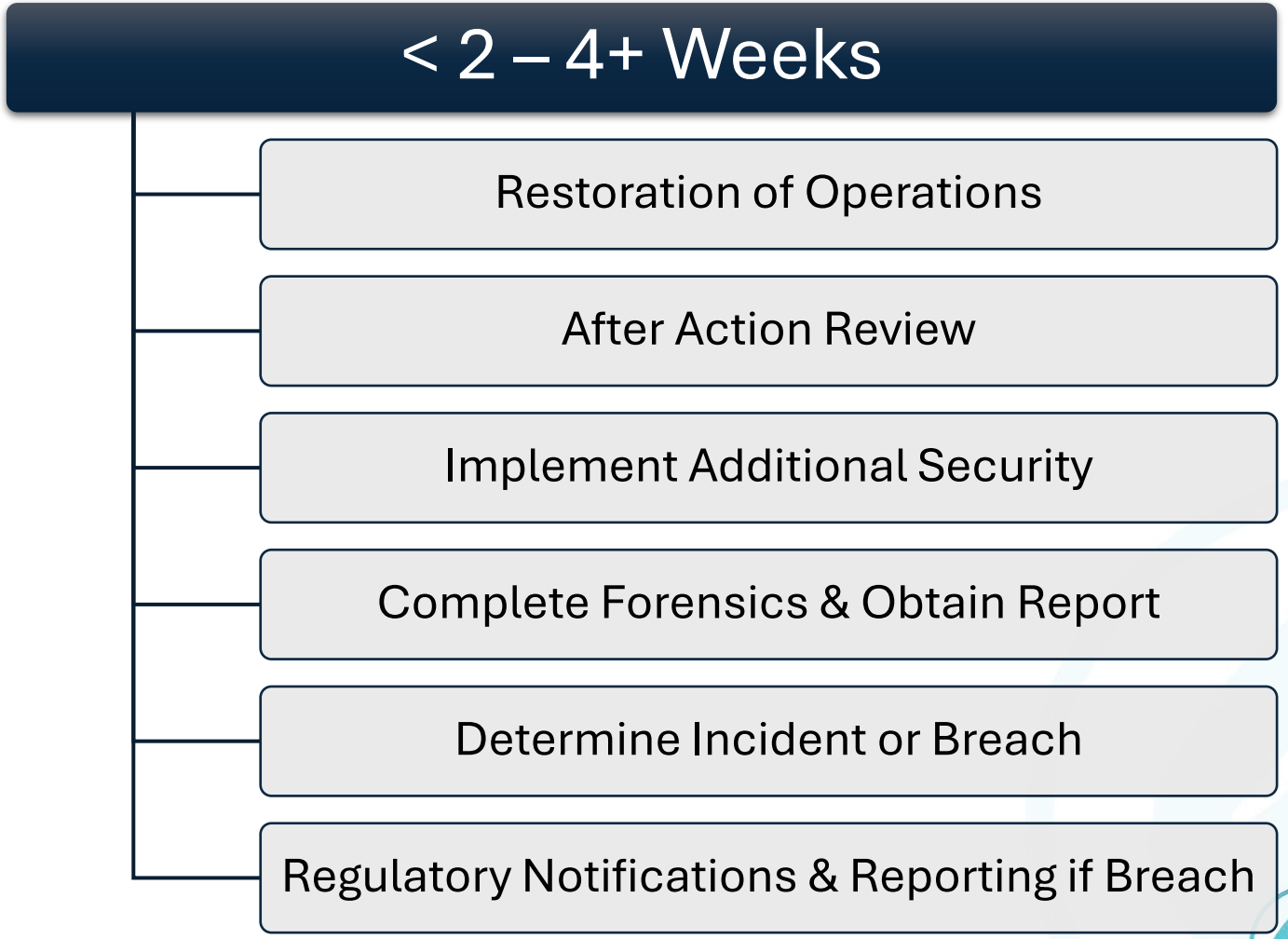
Impact

- CMS is backlogged with enrolling providers and switching clearinghouses for physician groups by at least 35 days.
- 100’s of Private practices bankrupt or near bankruptcy
- Massive alarm through the entire industry leaving questions about security, strategy, and backup plans

Advanced Institute for Anesthesia Billing & Practice Management

Strategies Going Forward

Ransomware Timeline



Advanced Institute for
Anesthesia Billing &
Practice Management

Ransomware Timeline

Advanced Institute for
Anesthesia Billing &
Practice Management

Critical Thinking

- Will another cyber attack occur in healthcare? Yes. Yes, it will.
- Have you done a cyber security check on your company?
  - Encryption standards – 256-bit encryption is the standard
  - Authentication standards
  - Training
  - Notifications
  - Insurance
  - Legal
- Do you have a cyber attack plan in place?

Advanced Institute for Anesthesia Billing & Practice Management

Process Improvement

Lean

- Efficiencies

Six Sigma

- Perfect

- Authentication
- Training Employees
- Cyber Attack Plan

Advanced Institute for Anesthesia Billing & Practice Management

HIPAA encryption standards12345:

- The minimum standard recommended by NIST is AES 128-bit encryption.
- While HIPAA does not specify specific encryption protocols, organizations can use NIST recommendations, including Advanced Encryption Standard (AES), OpenPGP, and S/MIME.
- Covered entities should implement standards and methodologies that adequately protect sensitive information.
- NIST recommends the use of AES 128, 192, or 256-bit encryption.

QUESTIONS?