PONDURANCE

Compliance in a Time of Crisis

diagnotes®
Patient care. Anywhere.

1

Hancock Health is an independent, 68-bed, full-service health system with:

- $150M annual revenue
- 1,200 employees
- 150 active medical staff members
- 20+ locations including a multi-site
- Multi-specialty physician practice
- Two diagnostic centers
- Cancer center
- Two wellness centers

2

Proactive Approach to IT and Workflow

The Gold Standard

- Best Equipment
- Best Software
- Best People
- Best Processes

"You might do the thing all the people do. But whatever you think is good enough is not. It's worth [it] to get the best stuff out there."
- Steve Long, President & CEO of Hancock Health

3

Anatomy of a Crisis

Technical and Clinical Conditions and Responses

- Pre-Incident Conditions
- The Incident
- The Response
- The Legal Analysis
- Preparing for an Incident
- Lessening the Likelihood of an Incident

Personal healthcare information is 10 times more valuable on the black market than retail information.

4

Pre-Incident Conditions

Pre-Incident Conditions

- Most wired x 3
- Comprehensive HIPAA privacy and security program
- Senior clinical Support for 'culture of communication'
- Board and C-suite support for privacy and security
- Area ERs on diversion due to high census of flu patients
- Heading into a holiday weekend
- Inclement weather approaching

5

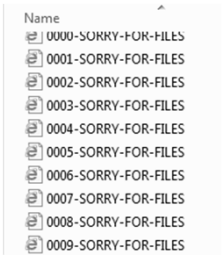
The Incident

Thursday, January 11, 2018

- **Thursday at 9:30 PM:** Messages began appearing on PC screens in the hospital indicating that the system was encrypted with SamSam ransomware
- **Decryption keys could be purchased** with four Bitcoin
- **Hancock was given one week to pay,** or data would be encrypted permanently
- **Message included step-by-step instructions** for obtaining the decryption keys

6

What it Looked Like…



7

The State of Affairs

No internet access meant:

- No EHR
- No landline phones
- No Outlook email

8

Guiding Principles for the Response

Three priorities:

1. Patient safety
2. Security of patient information
3. Time to restoration

9

Response Steps

Each step is critical for optimal results:

1. Activate Disaster Response Plan
2. Initiate downtime procedures and stabilize patient care processes
3. Contact key parties: legal counsel, IT forensics, FBI
4. Initiate IT forensic investigation
5. To pay or not to pay?

10

Step 1: Activate Disaster Response Plan

Begin the shut down.

- Manually turn off more than 1,200 units
- Post signs at all facilities stating computers must stay off

Incident command center established by executive leadership

- Non-essential staff called-off
- Communications by cell phone, secure messaging and non-system email, *without compromising compliance!*
- Diagnotes used by Clinical leadership to communicate and coordinate care

diagnotes® Patient care. Anywhere. LIVEPROCESS Board Effect

11

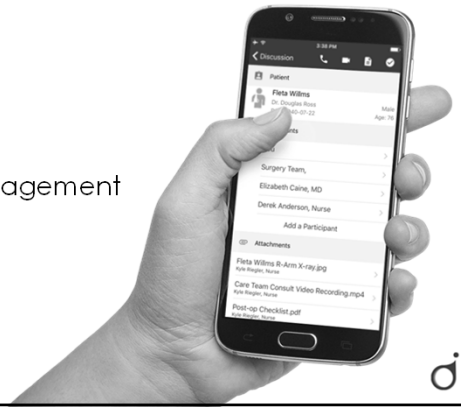
Step 1: Activate Disaster Response Plan (Cont'd)

Why Diagnotes?

Diagnotes is a cloud-hosted HIPAA-compliant platform that facilitates real-time communication and collaboration between and among healthcare professionals, administrators, providers and patients.

- Text discussions
- Voice memos
- Video chats
- Image sharing
- Call schedule management
- EHR integration

Mobile and Desktop Compatible



12

Step 2: Downtime Procedures and Patient Care

Keep calm and carry on.

- Ensured patient-facing equipment unaffected
- Patient care staff moved to paper documentation
- ER diversion only until processes established and stabilized
- Patient care continued throughout the incident

"Babies were born, surgeries were completed, patients were treated in ER and admitted, imaging and lab testing was performed. We did what a hospital does every day."

- Steve Long, President & CEO of Hancock Health

13

Step 3: Contact Key Parties

Assemble the A-Team

- Legal counsel contacted very early Friday morning
- Legal counsel engaged an experienced IT forensics firm
- Established schedule of calls to occur every two hours
- FBI contacted and included on calls. Their role is is advisory and investigative only.

PONDURANCE

HALL RENDER
KILLIAN HEATH & LYMAN

14

Step 4: Initiate Forensic Investigation

The Four Stages:

1. Identification
2. Containment
3. Eradication
4. Remediation

Failure to follow this process could result in incomplete resolution and continuing incident.

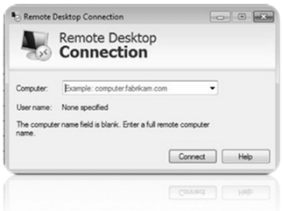
15

Forensic Investigation (cont.)

Review of logs determined:

Attackers deployed ransomware through a vendor's remote desktop protocol (RDP) access credentials

- Limited amount of access time
- No additional accounts created on network
- No lateral movement within network
- No evidence of ePHI exfiltration
- Ransomware was SamSam variant, which intelligence indicated seeks ransom payment only, not data acquisition



16

Step 5: To Pay or Not to Pay?

Factors to consider

- FBI recommends not paying, as a deterrent
- Fact-sensitive determination
- Risks of payment
- Success of business model relies on "integrity" of attackers
- Payment in form of Bitcoin
- Decryption keys vs. Manually restoring data

17

Legal Issues

State and Federal laws apply

State laws often focus on risk of identity theft

HIPAA presumes a breach when Privacy Rule is violated

- Is all ransomware an unauthorized access/disclosure?
- Can overcome presumption if able to document that there is a low probability that PHI has been compromised

Key Factors for ransomware incident:

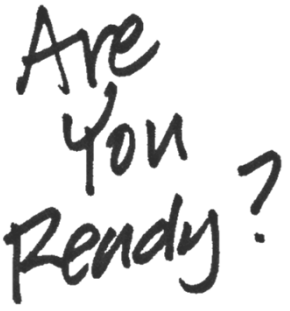
- Was ePHI or PII acquired or viewed?
- Was data availability compromised?

18

Be Prepared

Hope for the best. Plan for the worst.

- Develop an Incident Response Plan + Practice it!
- Nurture a Culture of Communication and strong organizational dynamics
- Obtain cyber liability insurance and audit vendor contracts to ensure proper protections
- Enable detailed system and application logging
- Utilize a cloud-based communications software like Diagnotes



19

Response Team Dynamics

Characteristics of an effective Incident Response Team:

- **Availability:** Requires complete dedication to the task.
- **Selflessness:** It's not about you, it is about getting it right.
- **Delegation:** Trust your team. You can't do it by yourself.
- **Honesty:** Truth is integral to this process.

20

Crisis Timeline *

Thursday
9:30 PM – Cyber-attack
11:00 PM – All systems shut down
Midnight – Incident Response Team in place

Friday
Early AM – Attorneys, IT forensics team in progress
Mid-day – Cylance installation in progress
Afternoon – Ransom decision made
Evening – Bitcoin procured

Saturday
Early AM – decryption keys acquired (i.e. ransom paid – 4 Bitcoin ~$55,000)
Mid-morning – File decryption begins

Sunday
Morning
- Servers & PCs operational
- Signs removed

Early evening – Critical systems on line

Monday
Most systems operational

Within a few weeks, all systems operational.
Some Outlook calendar files were unrecoverable.

** Includes regular updates to employees, medical staff, and Board of Trustees throughout*

21

Minimizing Risk

Lessening the likelihood of an incident

- Conduct enterprise-wide risk analysis
- Develop and implement remediation plan
- Regularly update and patch software and systems
- Implement multi-factor authentication
- Implement a vendor management program
- Conduct regular workforce training
- Obtain independent third-party penetration testing
- Implement managed security services to monitor IT activity, vulnerabilities and risks
- Install AI-enabled software that can work offline
- Enable some level of system logging to assist in a forensic investigation (if needed)

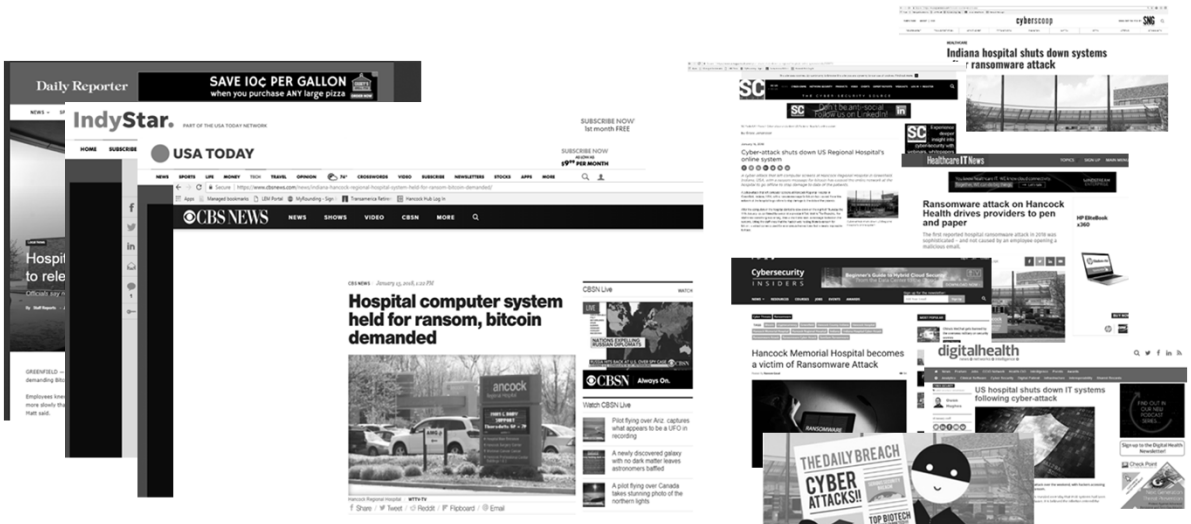
22

Why Hancock is Unique

Making lemonade

- ✓ Hancock was more prepared than many organizations are for an attack
- ✓ They are transparent and generously tell their story (and allow us to tell it) to educate other healthcare organizations that might be future targets of an attack
- ✓ Hancock's long-term commitment to clinical communication and care coordination meant they had more options during a crisis without comprising security and compliance standards
- ✓ The health of their organizational structure was tested and was an important asset during the investigation and recovery.
- ✓ They retained their sense of humor.

23



The Aftermath

24

Thank you!

Dave Wortman
CEO, Diagnotes
dwortman@diagnotes.com

Ron Pelletier
Founder, Pondurance
Ron.pelletier@pondurance.com

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.

25