# 405(d) Program Presents:

# A Case Study of "Cancer Care in the Wake of a Cyber Attack"

## Aligning Health Care Industry Security Approaches

- **Nate Couture-** Chief Information Security Officer at the University of Vermont Health Network
- **Erik Decker-** AVP and CISO at Intermountain and 405(d) Industry Co-Lead
- **Julie Chua-** GRC Director at the U.S. Department of Health and Human Services (HHS) and 405(d) Federal Co-Lead
- **Laura Wolf-** Director, Division of Critical Infrastructure Protection at U.S. Department of Health and Human Services (HHS)
- **David Ring-** Section Chief Cyber Engagement and Intelligence Section, Cyber Division, Federal Bureau of Investigation (FBI)
- **Josh Corman-** Chief Strategist, Cybersecurity and Infrastructure Security Agency (CISA)

# Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches.  The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole.  All Task Group Members have been invited to contribute this webinar series.

- This Webinar is being recorded and will be available for future viewing
- A note for media: While this event is open to the public, we would like to direct any media representatives to contact the public affairs office of whichever representative you have questions for to receive an official statement on behalf of the organization and refrain from quoting panelists during this event directly.

# 405(d) Events and Announcements

- **October**
  - Cybersecurity Awareness Month!
- **November**
  - National Critical Infrastructure Security and Resilience Month!
  - 405(d) Post 11/18
- **December**
  - Spotlight Webinar!  Date and topic TBD

**Email: CISA405d@hhs.gov**

**Social Media: @Ask405d LinkedIn, Twitter, Facebook, Instagram**

# Agenda

| Time | Topic | Speaker |
|---|---|---|
| *5 minutes* | Opening Remarks and Introductions | Chris Bollerer and Julie Chua, HHS |
| *20 Minutes* | Case study of UVM Ransomware Attack Overview | Nate Couture-Chief Information Security Officer at the University of Vermont Health Network |
| *5 Minutes* | Q&A | Nate Couture-Chief Information Security Officer at the University of Vermont Health Network |
| *15 Minutes* | Federal Agency Introductions and Role in a Cyber attack | **Laura Wolf-** Director, Division of Critical Infrastructure Protection at U.S. Department of Health and Human Services (HHS)<br>**David Ring-** Section Chief Cyber Engagement and Intelligence Section, Cyber Division, Federal Bureau of Investigation (FBI)<br>**Josh Corman-** Chief Strategist, Cybersecurity and Infrastructure Security Agency (CISA) |
| *30 Minutes* | Panel Discussion | All |
| *10 Minutes* | Q&A | All |
| *5 Minutes* | Closing | 405(d) Team |

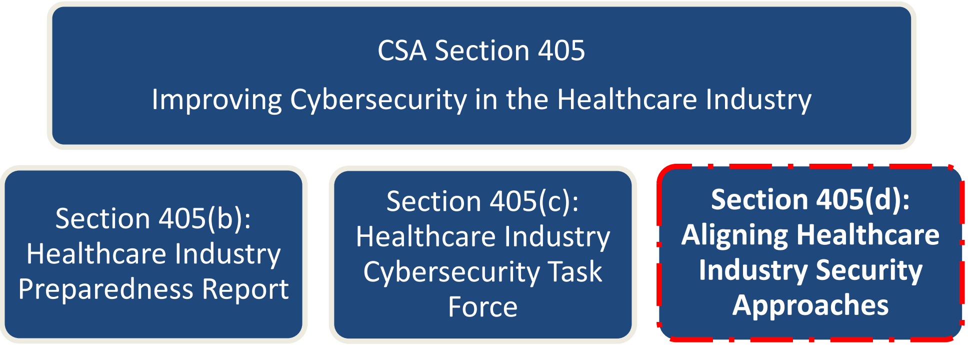
# A Message from Chris Bollerer
# Acting Chief Information Security Officer
# U.S. Department of Health and Human Services

# Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of “Aligning Health Industry Security Approaches” by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



CSA Section 405

Improving Cybersecurity in the Healthcare Industry

Section 405(b): Healthcare Industry Preparedness Report

Section 405(c): Healthcare Industry Cybersecurity Task Force

**Section 405(d): Aligning Healthcare Industry Security Approaches**

# 405(d) Resources

## 405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over 50 awareness products which organizations across the HPH sector can leverage.

## 405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

CYBERSECURITY TOWN HALL EVENT

October 22-23

PATIENTS TRUST US WITH THEIR LIVES, BUT DO WE PROTECT THEM FROM CYBER THREATS?

Join UChicago Medicine and United States Health and Human Services 405(d) to discuss the five main cybersecurity threats facing the healthcare industry and leading practices to mitigate them.

Town Hall Events:
Practitioners and Practice Managers:
10/22/19 1:30pm-3:00pm
10/23/19 9:00am-10:30am

IT Professionals:
10/22/19 3:30pm-5:00pm
10/23/19 11:00am-12:30pm

Telework During COVID-19 Good Practices To Protect From Cyberattacks

## 405(d) Social Media

The 405(d) Program is now live on LinkedIn Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

## Guest Webinars

The 405(d) program offers "Guest Webinars" to healthcare organizations where we provide information on the HICP Publication, 405(d) resources, how to engage your co-workers, and more

## SBARs

The 405(d) SBAR is a timely, event-oriented document to help healthcare organizations react and relate to current cyber events.

# Case study of UVM Ransomware Attack Overview

Nate Couture- Chief Information Security Officer at the University of Vermont Health Network

THE
University of Vermont
MEDICAL CENTER

# October 28, 2020

October 28th, 2020 seemed like a normal day at the University of Vermont Medical Network until a Ransomware Attack occurred.

Clinical impact perspective:

- **Loss of access to network intranet servers, email communications, and clinical systems.**

- **Electronic medical record (EMR) protectively taken offline resulting in loss of access to production records including laboratory, pathology, pharmacy, and radiology.**

Technical impact perspective:

- **1300 servers offline, hundreds of applications impacted, and over 5000 endpoints infected.**

- **Containment actions to disable internet, VPNs, and integrations and proactively take the EHR offline.**

# Immediate Steps Taken

Although UVMMC had disaster recovery and business continuity plans in place for all major systems as well as third-party consultant on retainer to provide guidance in the event of a major cybersecurity incident, it was clear within hours that this was a severe ransomware attack with the potential to disrupt institutional provision of life-saving care.

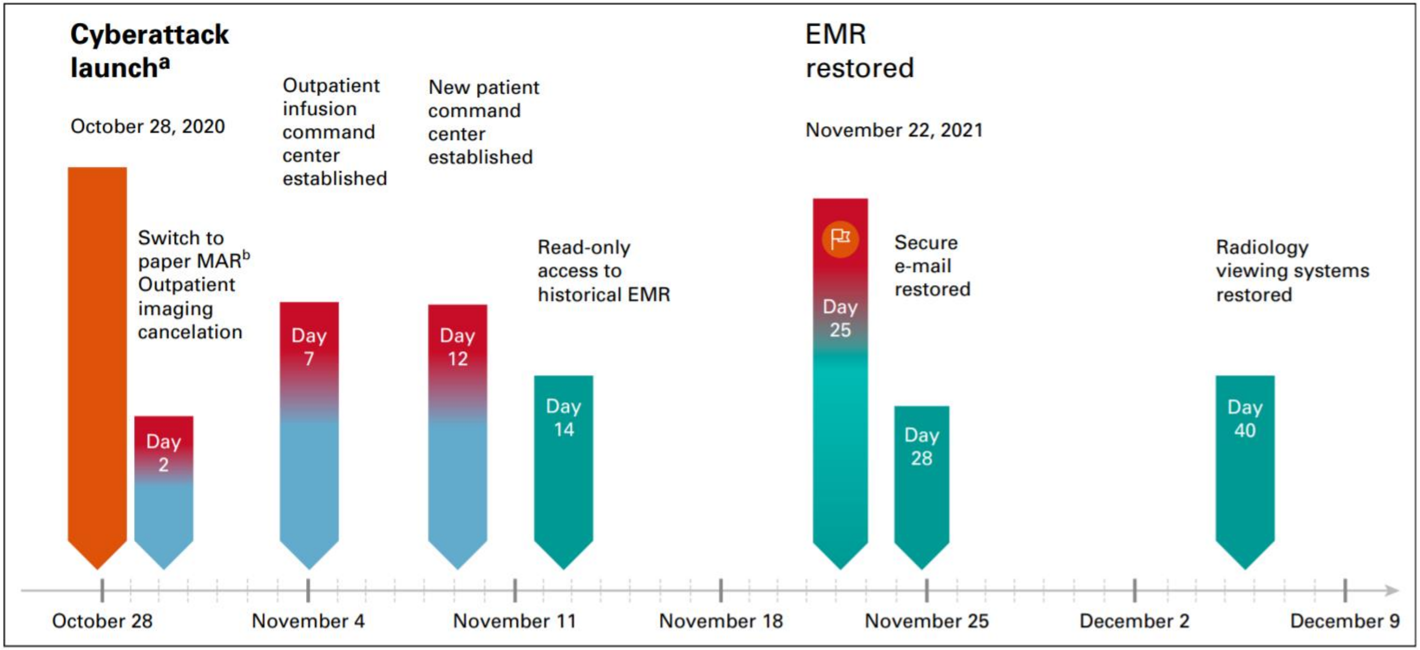
- Federal and local Law enforcement notified
- IT incident command center and a broader hospital command center to manage the operational impacts and communication stood up
- Cyber Incident Response Process initiated and external forensics and response firm active.

**Damage Containment Measures Taken:**

- Taking the EMR offline
- Cut off all internet and other access both to and from UVMMC
- Severed connections to affiliates and other partners
- Deployed EDR agents to all endpoints
- Blocked traffic at internal segments

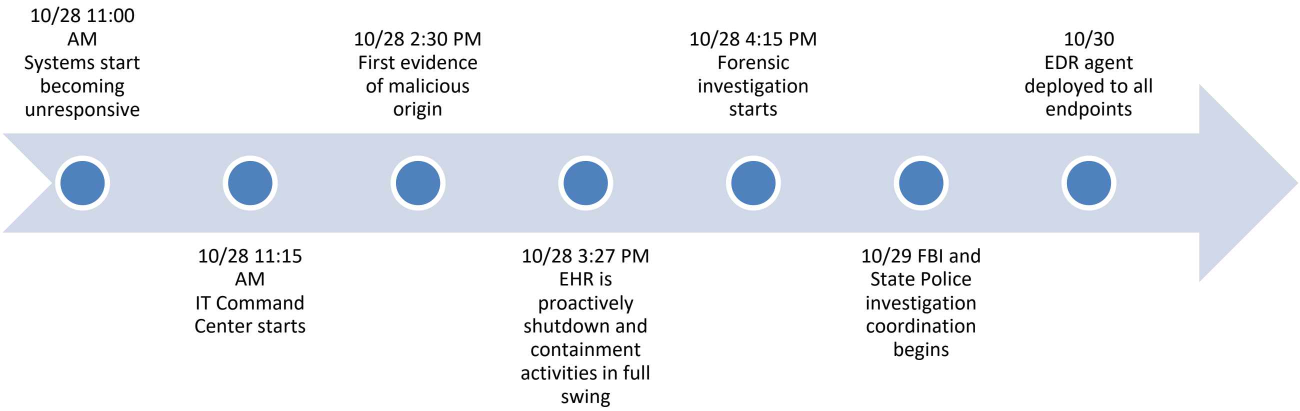
# Cyberattack Response Timeline

## Clinical View


Cyberattack launch[a]
October 28, 2020
Switch to paper MAR[b] Outpatient imaging cancelation
Day 2
Outpatient infusion command center established
Day 7
New patient command center established
Day 12
Read-only access to historical EMR
Day 14
EMR restored
November 22, 2021
Day 25
Secure e-mail restored
Day 28
Radiology viewing systems restored
Day 40
October 28
November 4
November 11
November 18
November 25
December 2
December 9

# Cyberattack Response Timeline

## IT View



10/28 11:00 AM
Systems start becoming unresponsive

10/28 11:15 AM
IT Command Center starts

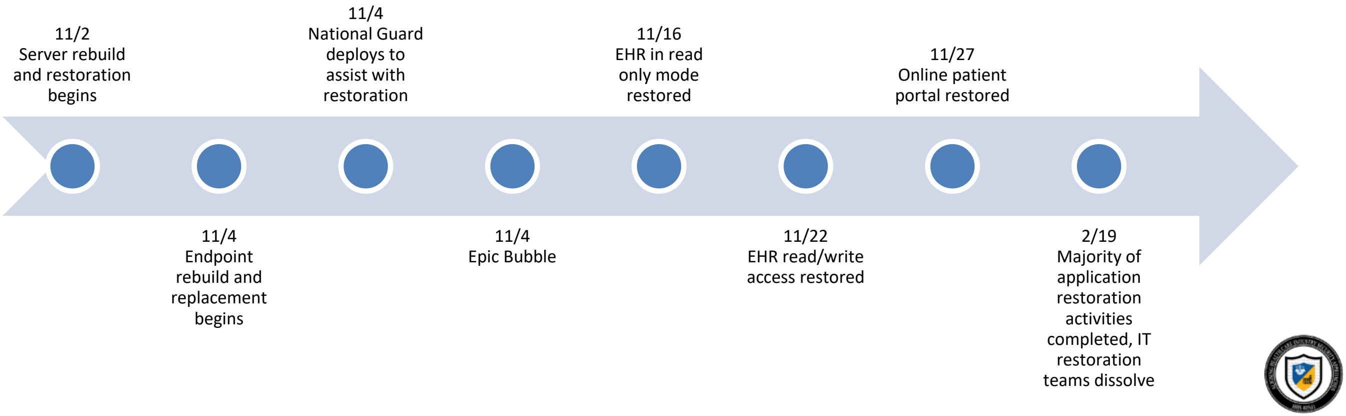
10/28 2:30 PM
First evidence of malicious origin

10/28 3:27 PM
EHR is proactively shutdown and containment activities in full swing

10/28 4:15 PM
Forensic investigation starts

10/29 FBI and State Police investigation coordination begins

10/30
EDR agent deployed to all endpoints



11/2
Server rebuild and restoration begins

11/4
Endpoint rebuild and replacement begins

11/4
National Guard deploys to assist with restoration

11/4
Epic Bubble

11/16
EHR in read only mode restored

11/22
EHR read/write access restored

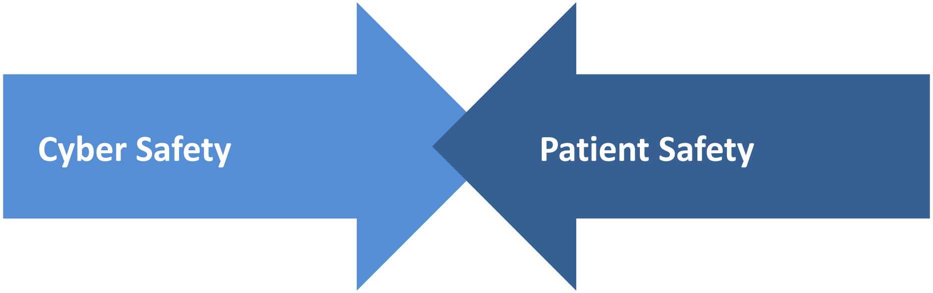
11/27
Online patient portal restored

2/19
Majority of application restoration activities completed, IT restoration teams dissolve

# Major Impacts to Oncology Outlined in Study

- The loss of communication channels and the loss of the individualized EMR chemotherapy plan templates driving nursing and pharmacy processes to enable the safe delivery of systemic therapies to our cancer patient population
- Loss of a reliable encrypted email communications platform challenged efforts to organize and coordinate our response as the COVID-19 pandemic, and prevented regular, large, and in-person meetings

**Given data documenting the impact of treatment delay on survival in select cancer patient populations and the acute treatment toxicities managed as an outpatient, the sustained effects of the cyberattack presented specific challenges related to oncology care.**

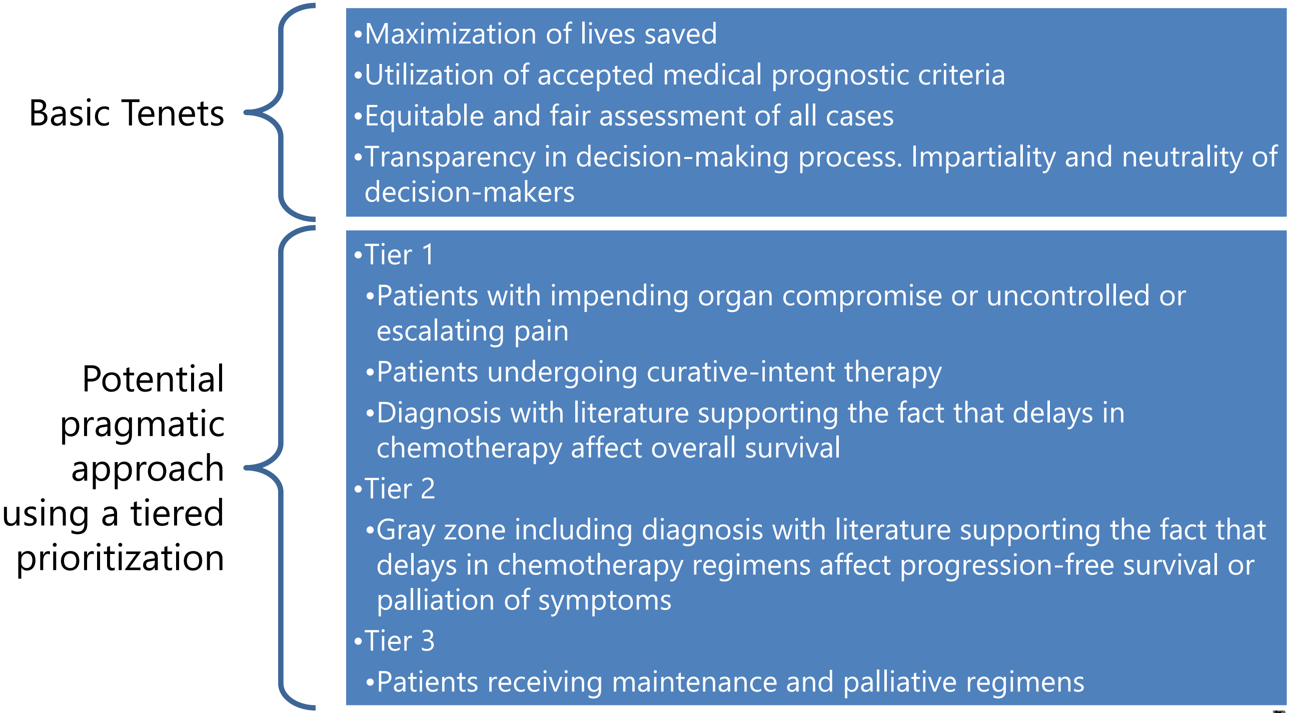


Cyber Safety

Patient Safety

# Making Ethical Decisions and Continuing Care in the Wake of a Cyber Attack

During a major cyber attack serious decisions of patient care must be made. Below is an template of the value-based principles leadership followed to ensure pragmatic processes for ethical allocation of cancer care during the cyber attack.



Basic Tenets

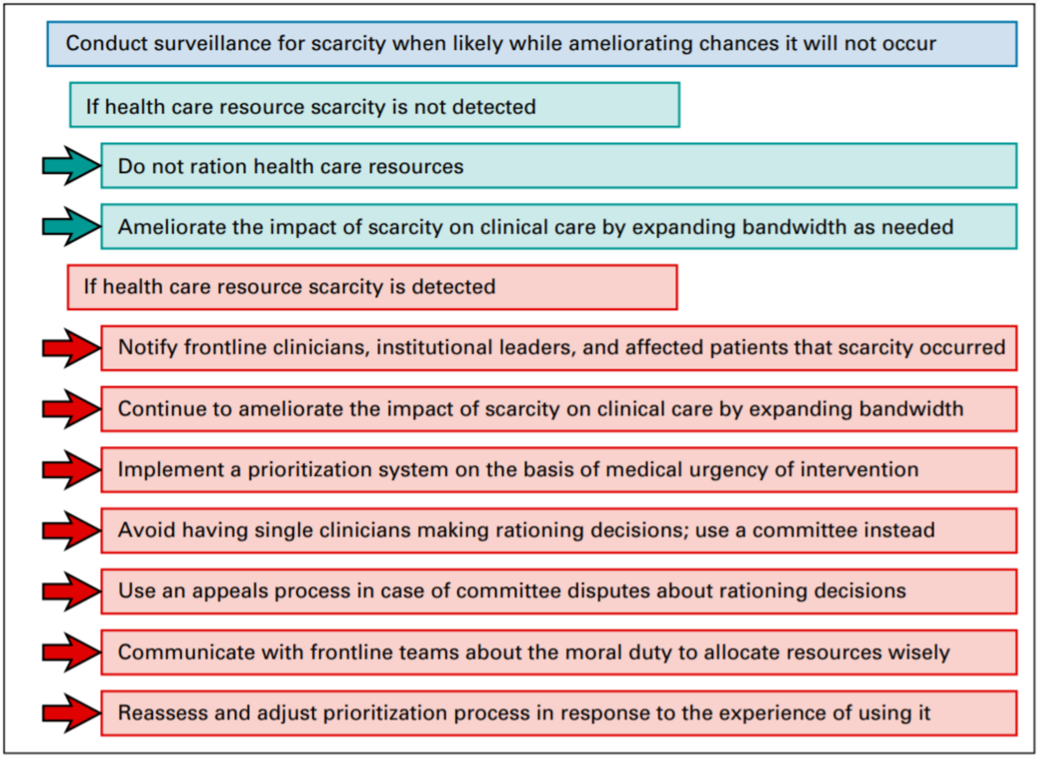
- Maximization of lives saved
- Utilization of accepted medical prognostic criteria
- Equitable and fair assessment of all cases
- Transparency in decision-making process. Impartiality and neutrality of decision-makers

Potential pragmatic approach using a tiered prioritization

- Tier 1
  - Patients with impending organ compromise or uncontrolled or escalating pain
  - Patients undergoing curative-intent therapy
  - Diagnosis with literature supporting the fact that delays in chemotherapy affect overall survival
- Tier 2
  - Gray zone including diagnosis with literature supporting the fact that delays in chemotherapy regimens affect progression-free survival or palliation of symptoms
- Tier 3
  - Patients receiving maintenance and palliative regimens

# Continuing Care in a Ransomware Attack

To enact the principles on the previous slide, oncology leadership enacted a simple, pragmatic, and transparent process in collaboration with ethics leadership summarized below.



Conduct surveillance for scarcity when likely while ameliorating chances it will not occur

If health care resource scarcity is not detected

- Do not ration health care resources
- Ameliorate the impact of scarcity on clinical care by expanding bandwidth as needed

If health care resource scarcity is detected

- Notify frontline clinicians, institutional leaders, and affected patients that scarcity occurred
- Continue to ameliorate the impact of scarcity on clinical care by expanding bandwidth
- Implement a prioritization system on the basis of medical urgency of intervention
- Avoid having single clinicians making rationing decisions; use a committee instead
- Use an appeals process in case of committee disputes about rationing decisions
- Communicate with frontline teams about the moral duty to allocate resources wisely
- Reassess and adjust prioritization process in response to the experience of using it

# Positive Impacts of Command Centers

To continue effective healthcare delivery in real-time without access to EMR and intranet, several "Command Centers" were set up. See below for an example of the importance of the Outpatient Command Center in Oncology and what it accomplished.

1. Centralized mechanism to gather data: A paper database was created for all patients receiving treatment during downtime and individual paper charts for each patient in need of therapy

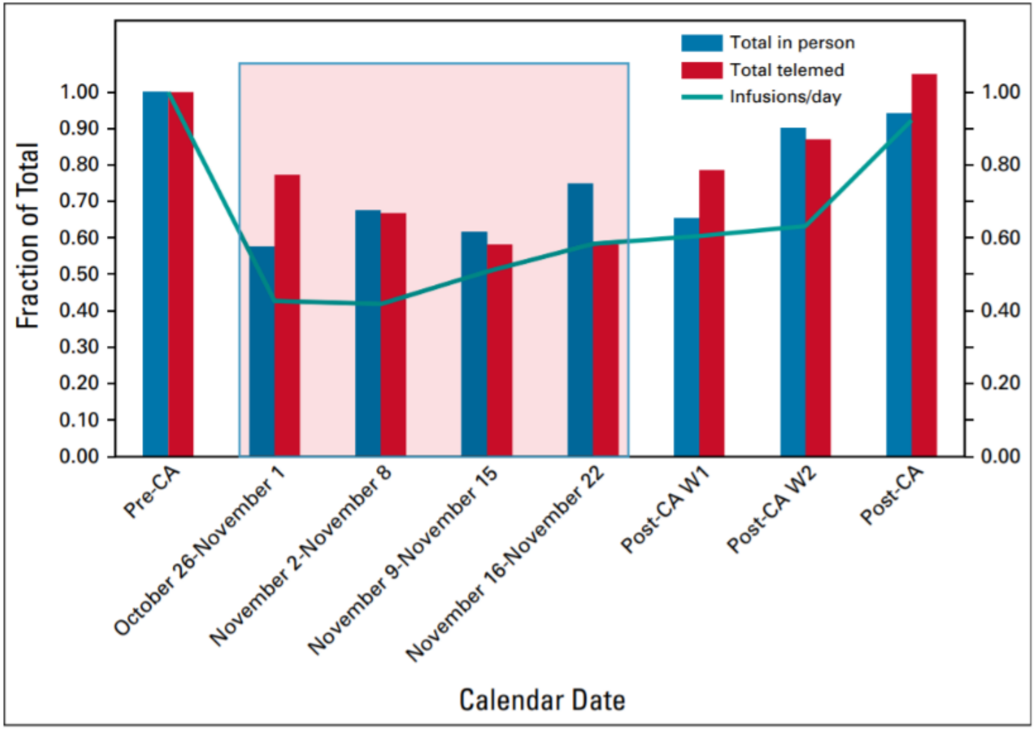
2. Coordinating body for prioritization: A list of patients with missed or upcoming therapy was provided to each physician for patient stratification

3. Expanding operating hours

4. Managed network referrals: On the basis of stratification and resource capability, some patients were referred to network affiliates sites to complete their chemotherapy.

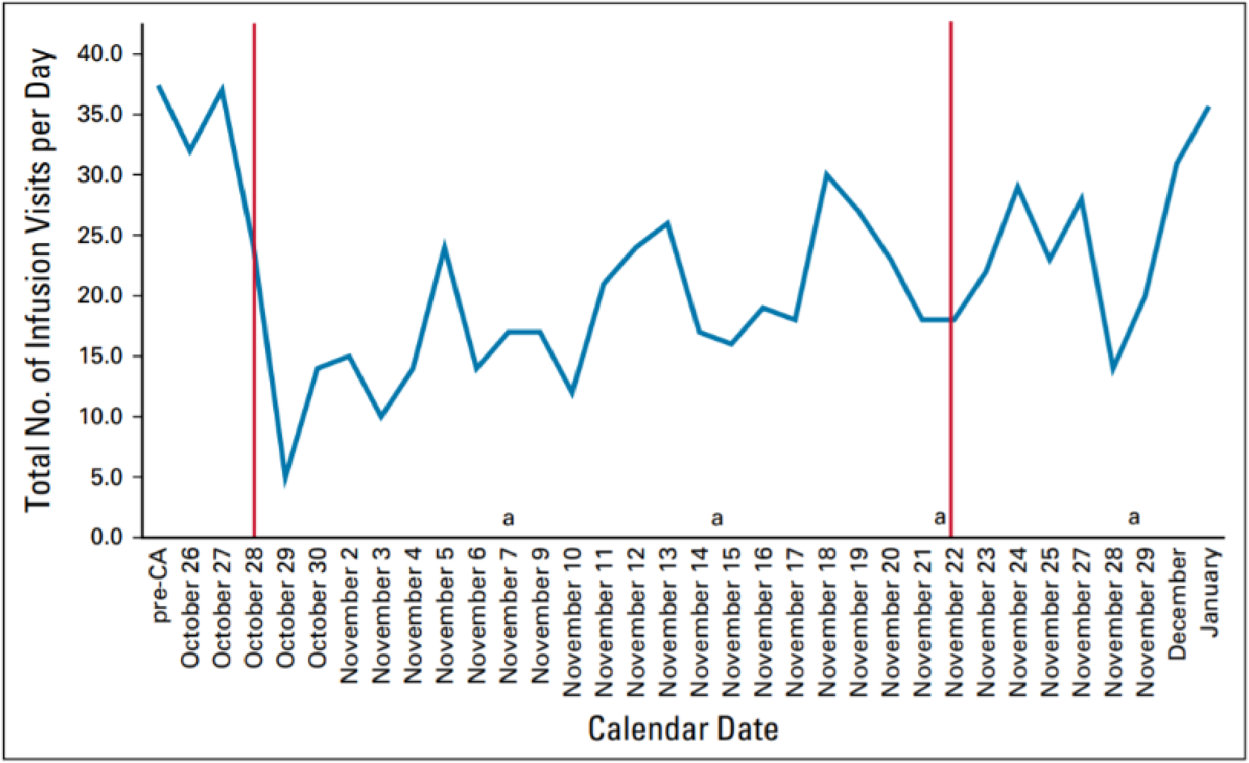
# Cyberattack ERM Impacts to the Oncology Department

In total, compared with the preceding 2 months, the cyberattack resulted in an 41% decrease in total outpatient volume including a 39% decrease in new patient visits on the basis of weekly totals averaged over the cyberattack period. Both telemedicine and in-person visits were equally affected.



# Cyberattack ERM Impacts to the Oncology Department Cont.

In particular, infusion center visits dropped initially by 63% in the first week before rebounding gradually in response to corrective actions taken.



# Conclusion

In conclusion, many lessons were learned in our response to the cyberattack crisis including the immediate need for updated standardized processes to address the host of challenges that we faced with loss of EMR and communication systems and the realization that **IT cannot be our only solution in the face of a cyberattack.**

**Clinical Take-Aways:**

- Backup of physical copies of all forms and systemic therapy templates is essential as well as access to basic patient information and secure platforms for all communication
- Coordination with hospital administration early on during the attack was key to mobilize resources to stand up necessary command centers that can respond to the most significant challenges that we faced in the safe delivery of systemic therapies to established patients and respond to the immediate needs of patients with a new cancer diagnosis

**IT Take-Aways:**

- Understanding of application priorities and interdependencies
- Prepare for interim solutions, but also prepare to identify and vet interim solutions during an event
- Be prepared to answer “How can I help?”
- Relationships, communication, and coordination early and always

# Questions?

# FBI's Role In A Ransomware Attack

David Ring
Section Chief
Cyber Engagement and Intelligence Section

# FBI Cyber Strategy

***FBI Cyber Mission -*** To impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building on a century of innovation

***Incident Response:*** The FBI provides subject matter expertise and technical resources through our local field offices and our Cyber Action Teams (CAT) and leverages other state, local, private sector partners to assist victims and move forward investigations.

***Pledge to Victims*****:** The FBI will always treat victims with dignity and respect, protecting their privacy and data, and rigorously adhering to the U.S. Constitution, applicable laws, regulations, and policies, and the FBI's Core Values. In pursuing our mission, we recognize that we will encounter unique and novel issues related to privacy and handling of sensitive data.

***Private Sector Engagement*****:** Focused on driving substantive collaboration between the FBI and private sector to better integrate the insight, capabilities, and information maintained outside of government into FBI cyber investigations and intelligence, while sharing back with private sector that information enriched with additional insight gleaned through FBI investigations.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

# Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**

Secure and resilient infrastructure for the American people.

**MISSION**

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

## OVERALL GOALS

**GOAL 1**

### DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

**GOAL 2**

### SECURE TOMORROW

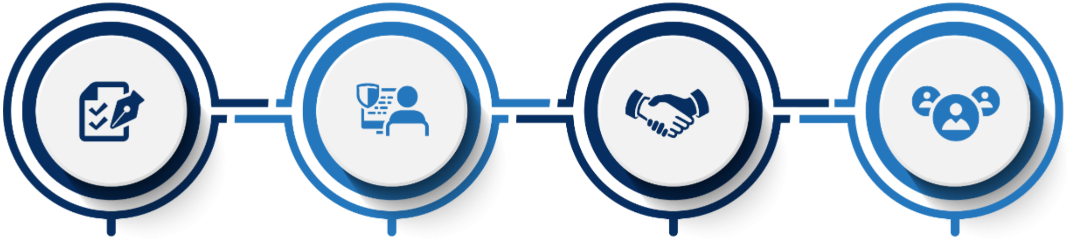
Strengthen critical infrastructure and address long-term risks

months | years | decades

# HHS Office of the Assistant Secretary for Preparedness and Response

ASPR leads the nation’s medical and public health preparedness for, response to, and recovery from disasters and public health emergencies. For more information, visit: http://aspr.hhs.gov

**ASPR’s Role in Cyber Incident Response:** Support continuity of national critical functions for Healthcare and Public Health



Perform contextual risk and impact assessment

Maintain situational awareness across government and industry partners

Support unity of effort among federal partners

Promote and coordinate information sharing

**Sign Up**

Bulletins and informational calls – sign up here: https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx

# Panel Discussion

# Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

# A **CALL TO ONE** IS A **CALL TO ALL**

## HHS

To contact the Assistant Secretary for Preparedness and Response (ASPR):
**Email:** CIP@hhs.gov

To contact Health Sector Cybersecurity Coordination Center (HC3):
**Email:** HC3@hhs.gov

## FBI

Report incidents to your local FBI Field Office, or contact:
**Email:** cywatch@fbi.gov
**Online:** IC3.gov
**Phone:** 1 (855) 292-3937

## CISA

**Email:** Central@cisa.dhs.gov
**Online:** us-cert.cisa.gov/report
**Phone:** 1 (888) 282-0870

# Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

***Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)***

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.