Cybersecurity, Privacy & Secure Data Exchange



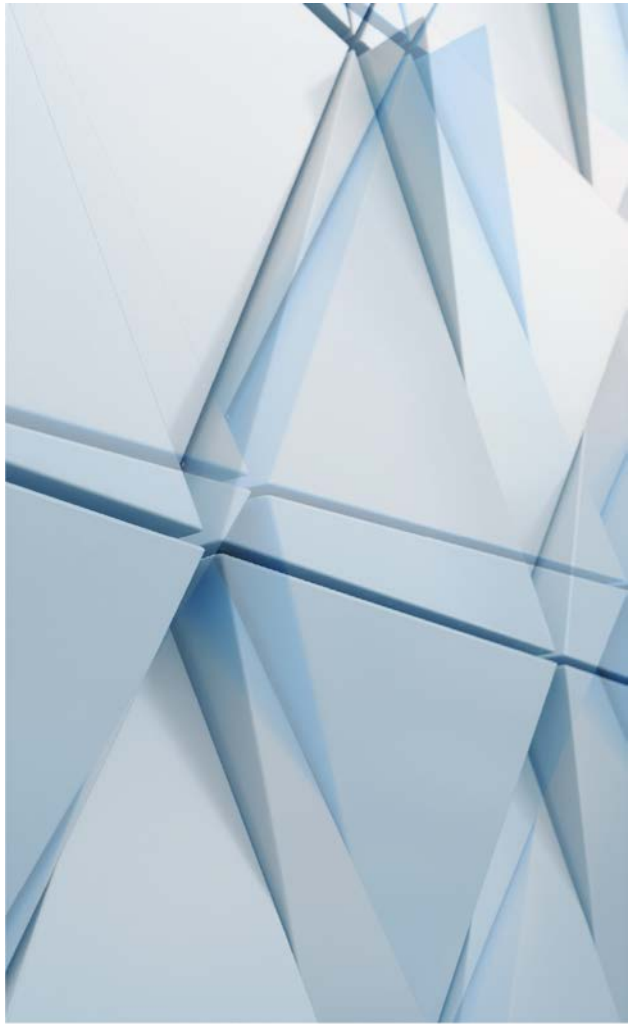
Lee Barrett, Executive Director, CEO
lbarrett@ehnac.org

EHNAC™

July 2022

Agenda

- Breach, Ransomware Landscape
- The Interoperability Factor
- 21st Century Cures Act - TEFCA
- The Carin Influence
- Program Options: TDRAAP and TNAP
- Cyber Hygiene Scorecard
- Questions & Answers



THE BREACH, CYBER-RANSOMWARE LANDSCAPE



Recent Stats

EHNAC



The Cyber Stats

EHNAC

Key findings

The key findings described here are based on IBM Security analysis of the research data compiled by the Ponemon Institute.

10%

Increase in average total cost of a breach, 2020-2021

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.

Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the history of this report. Costs were significantly lower for some of organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI and automation, zero trust and cloud security.

Note: Cost amounts in this report are measured in U.S. dollars.

$1.07m

Cost difference where remote work was a factor in causing the breach

Remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach.

The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor. The percentage of companies where remote work was a factor in the breach was 17.5%. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely. IT changes such as cloud migration and remote work increased costs, yet organizations that did not implement any digital transformation changes as a result of COVID-19 experienced $750,000 higher costs compared to the global average, a difference of 16.6%.

11

Consecutive years healthcare had the highest industry cost of a breach

Healthcare organizations experienced the highest average cost of a data breach, for the eleventh year in a row.

Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Costs varied widely across industries, and year over year. Costs in the energy sector decreased from $6.39 million in 2020 to an average $4.65 million in 2021. Costs surged in the public sector, which saw a 78.7% increase in average total cost from $1.08 million to $1.93 million.

The Cyber Stats (cont)

EHNAC

38%

Lost business share of total breach costs

Lost business represented the largest share of breach costs, at an average total cost of $1.59M.

Lost business represented 38% of the overall average and increased slightly from $1.52 million in the 2020 study. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation.

$180

Per record cost of personally identifiable information

Customer personally identifiable information (PII) was the most common type of record lost, included in 44% of breaches.

Customer PII was also the costliest record type, at $180 per lost or stolen record. The overall average cost per record in the 2021 study was $161, an increase from $146 per lost or stolen record in the 2020 report year.

20%

Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

Business email compromise (BEC) was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million).

The Cyber Stats (cont)

EHNAC

$4.62m

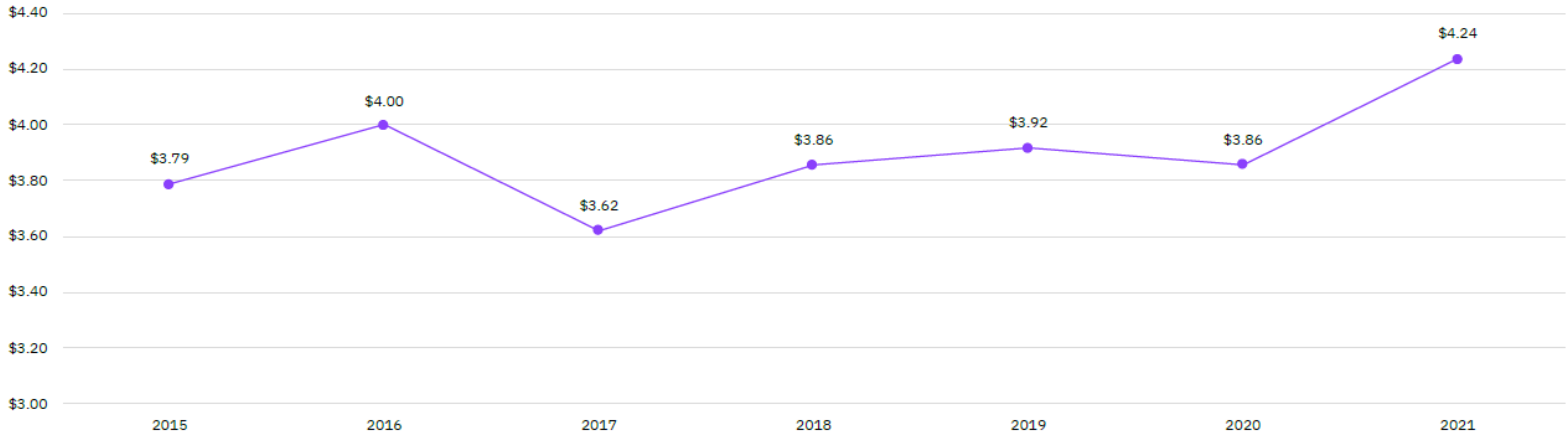
Average
total cost of a
ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Ransomware attacks cost an average of $4.62 million, more expensive than the average data breach ($4.24 million). These costs included escalation, notification, lost business and response costs, but did not include the cost of the ransom. Malicious attacks that destroyed data in destructive wiper-style attacks cost an average of $4.69 million. The percentage of companies where ransomware was a factor in the breach was 7.8%.

Average total cost of a data breach

Measured in US$ millions

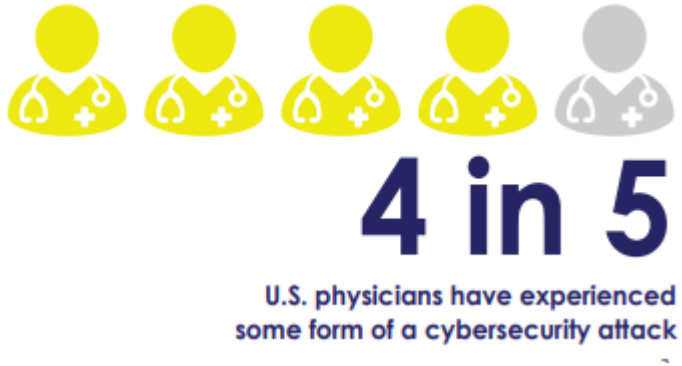


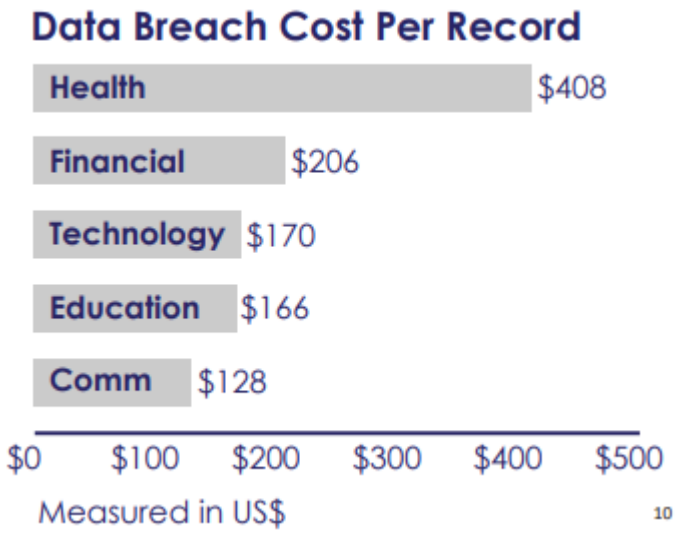
The average total cost of a data breach increased by the largest margin in seven years.

Data breach costs increased significantly year-over year from the 2020 report to the 2021 report, increasing from $3.86 million in 2020 to $4.24 million in 2021.

The increase of $0.38 million ($380,000) represents a 9.8% increase. This compares to a decrease of 1.5% from the 2019 to 2020 report year. The cost of a data breach has increase by 11.9% since 2015.

HHS 405(d) Cybersecurity Info. Sharing Act (CISA)

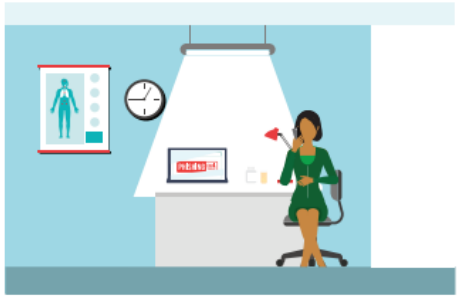




What are the Threats?

Threat: E-mail Phishing Attack		
Vulnerabilities Lack	**Impact**	**Practices to Consider**
of awareness training Lack of IT resource for managing suspicious e-mails Lack of software scanning e-mails for malicious content or bad links Lack of e-mail detection software testing for malicious content Lack of e-mail sender and domain validation tools	Loss of reputation in the community (referrals dry up, patients leave the practice) Stolen access credentials used for access to sensitive data Erosion of trust or brand reputation Potential negative impact to the ability to provide timely and quality patient care Patient safety concerns	Be suspicious of e-mails from unknown senders, e-mails that request sensitive information such as PHI or personal information, or e-mails that include a call to action that stresses urgency or importance (1.S.B) Train staff to recognize suspicious e-mails and to know where to forward them (1.S.B) Never open e-mail attachments from unknown senders (1.S.B) Tag external e-mails to make them recognizable to staff (1.S.A) Implement incident response plays to manage successful phishing attacks (8.M.A) Implement advanced technologies for detecting and testing e-mail for malicious content or links (1.L.A) Implement multifactor authentication (MFA) (1.S.A, 3.M.D) Implement proven and tested response procedures when employees click on phishing e-mails (1.S.C) Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)

Threat: E-mail Phishing Attack



Real-World Scenario:
Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.

Description:
E-mail phishing is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using e-mail. An inbound phishing e-mail includes an active link or file (often a picture or graphic). The e-mail appears to come from a legitimate source, such as a friend, coworker, manager, company, or even the user's own e-mail address. Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer or other computers within your network.[18]

Impact:
A pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.

Table 2 identifies vulnerabilities, impacts, and Practices to consider for e-mail phishing attacks.

Threat Quick Tips	
What to Ask?	On average, a person will receive about 80 e-mails per day. Knowing which are safe to open can get tricky if you are not asking yourself the following questions: • Do you know the sender? • Are there any spelling or grammatical errors, or any other indicators that the tone or style of the e-mail is off? • Before clicking on a link, did you hover over it to see the URL destination? • Do you know the sender, or are you suspicious of the e-mail? If in doubt, do NOT open any attachments. • What are my organization's processes for reporting suspicious e-mails?
When to Ask?	The best time to familiarize yourself with your organization's policies for reporting a suspicious e-mail is when you begin employment. Whenever you receive an e-mail that sounds too good to be true or that you were not expecting, verify it before opening it!
Who to Ask?	Check with colleagues to find out whether they received the same phishy e-mail. You can always seek the guidance of your IT security support team or similar point of contact. Talk to them to find out whether your account is protected with the proper security filters to ward off unwanted junk mail.

What are the Threats?

Threat: Ransomware Attack		
Vulnerabilities	**Impact**	**Practices to Consider**
Lack of system backup Lack of anti-phishing capabilities Unpatched software Lack of anti-malware detection and remediation tools Lack of testing and proven data back-up and restoration Lack of network security controls such as segmentation and access control	Partial or complete clinical and service disruption Patient care and safety concerns Expenses for recovery The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Ensure that users understand authorized patching procedures (7.S.A) Patch software according to authorized procedures (7.S.A) Be clear which computers may access and store sensitive or patient data (4.M.C) Use strong/unique username and passwords with MFA (1.S.A, 3.S.A, 3.M.C) Limit users who can log in from remote desktops (3.S.A, 3.M.B) Limit the rate of allowed authentication attempts to thwart brute-force attacks (3.M.C) Deploy anti-malware detection and remediation tools (2.S.A, 2.M.A, 3.L.D) Separate critical or vulnerable systems from threats (6.S.A, 6.M.B, 6.L.A) Maintain a complete and updated inventory of assets (5.S.A, 5.M.A) Implement a proven and tested data backup and restoration test (4.M.D) Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up (4.M.D) Implement proven and tested incident response procedures (8.S.A, 8.M.B) Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C) Develop a ransomware recovery playbook and test it regularly (8.M.B) Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Fact Sheet)

EHNAC

Threat: Ransomware Attack



Description:
The HHS Ransomware Factsheet, available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf, defines ransomware as follows: "Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so." Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats. For example, successful phishing attacks may lead to the installation of ransomware.

Real-World Scenario:
Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.

Impact:
A practitioner cannot view patient charts because of a ransomware attack that has made the EHR system inaccessible.

Table 3 identifies vulnerabilities, impacts, and Practices to consider for ransomware attacks.

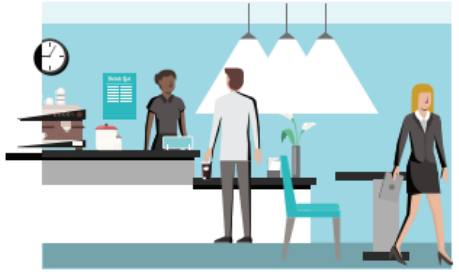
Threat Quick Tips	
What to Ask?	Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Be sure you know how to identify these phishing e-mails! Stay alert when any e-mail asks you to enter your credentials. As a proactive measure, check to see whether the computer and network to which you are connected have the proper intrusion prevention system or software in place. That means asking • Do I have a high-performance firewall? • Do I have my firewall configured to only allow certain ports to be open? • Is there training I should be aware of to understand my organization's security policies?
When to Ask?	Provide user awareness and compliance training during the onboarding process or when purchasing a new laptop or desktop equipment. If you discover that your computer has been infected, immediately disconnect from the network and notify your IT security team. Do not power off or shut down the computer or server, in case a volatile (RAM) memory image needs to be collected for forensics and incident response investigations.
Who to Ask?	Due to the severity and time sensitivity of ransomware attacks, it is in your best interest and that of your organization to always seek out professional IT security or a similar point of contact help when you think your computer is infected with ransomware.

What are the Threats?

Threat: Loss or Theft of Equipment or Data		
Vulnerabilities	**Impact**	**Practices to Consider**
Lack of asset inventory and control Lack of encryption; Data at rest is data stored on a hard drive at any location. Lack of physical security practices; open offices and poor physical access management, giving attackers opportunities Lack of simple safeguards such as computer cable locks to secure devices within office environments Lack of awareness that theft of IT assets from the office accounts for nearly as much as from cars Lack of effective vendor security management, including controls to protect equipment or sensitive data Lack of "End-of-Service" process to clear sensitive data before IT assets, including medical devices, are discarded or transferred to other users or other organizations	Inappropriate access to or loss of sensitive patient information occurs; may involve proprietary or confidential company information or intellectual property Theft or loss of unencrypted PHI or PII; may result in a data breach requiring notification to affected patients, relevant regulatory bodies, and the media Lost productivity Damage to reputation	Encrypt sensitive data, especially when transmitting data to other devices or organizations (4.S.B, 4.M.C) Implement proven and tested data backups, with proven and tested restoration of data (4.M.D) Acquire and use data loss prevention tools (4.M.E, 4.L.A) Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices (9.M.A) Promptly report loss/theft to designated company individuals to terminate access to the device and/or network (3.S.A) Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices such as laptops and USB/thumb drives (5.S.A) Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device (4.M.C) Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold (5.S.C, 5.M.D)

EHNAC

Threat: Loss or Theft of Equipment or Data



Description:
Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen, and they end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. From January 1, 2018, to August 31, 2018, the Office for Civil Rights received reports of 192 theft cases affecting 2,041,668 individuals. Although the value of the device represents one loss, far greater are the consequences of losing a device that contains sensitive data. In cases where the lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.

Real-World Scenario:
A physician stops at a coffee shop for a coffee and to use the public Wi-Fi to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop. The doctor returns to the table to find the laptop is gone.

Impact:
Loss of sensitive data may lead to a clear case of patient identity theft, and, with thousands of records potentially stolen, the physician's reputation could be at stake if all the patient records make it to the dark web for sale.

Table 4 identifies vulnerabilities, impacts, and Practices to consider for loss or theft of equipment or data.

Threat Quick Tips	
What to Ask?	Heading out on a business trip or a personal holiday? You need to follow the same, and maybe greater, security procedures as you do in the office. Make sure you know your organization's policy on removing equipment from the workplace by asking: • Can I travel with my equipment? • Can I take my equipment offsite to work remotely? • Are USB or other portable storage devices allowed? • Is the information on my computer or storage device encrypted? • Is there a secure virtual private network (VPN) that I can use, along with secure, password-protected Wi-Fi, to log into the network and work?
When to Ask?	As soon as you realize that your device or equipment has been stolen or misplaced, your supervisor and IT security professional should be notified immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.
Who to Ask?	Your IT security support staff or similar point of contact should be notified when a work device or equipment has been misplaced, lost, or stolen. The data saved on them are now compromised and susceptible to unauthorized access, dissemination, and use. This is a serious cyber breach and should be handled by trained IT security professionals.

What are the Threats?

Threat: Insider, Accidental or Intentional Data Loss		
Vulnerabilities Files containing sensitive data accidentally e-mailed to incorrect or unauthorized addressees Lack of adequate monitoring, tracking, and auditing of access to patient information on EHR systems Lack of adequate logging and auditing of access to critical technology assets, such as e-mail and file storage Lack of technical controls to monitor the e-mailing and uploading of sensitive data outside the organization's network Lack of physical access controls Lack of training about social engineering and phishing attacks	**Impact** Accidental loss of PHI or PII through e-mail and unencrypted mobile storage, resulting in reportable data breaches Reportable incidents involving patients who are victims of employees who inappropriately view patient information Financial loss from insiders being socially engineered into not following proper procedures Financial loss due to an employee inadvertently giving an attacker access to banking and routing numbers because the attacker used a phishing e-mail disguised as originating from the bank Patients given the wrong medicines or treatment because of incorrect data in the EHR	**Practices to Consider** Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors (1.S.B, 1.M.D) Implement and use workforce access auditing of health record systems and sensitive data (3.M.B) Implement and use privileged access management tools to report access to critical technology infrastructure and systems (3.M.C) Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads (4.M.E, 4.L.A)

Threat: Insider, Accidental or Intentional Data Loss



Description:
Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional.

An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, being the victim of an e-mail phishing attack is an accidental insider threat.

An intentional insider threat is malicious loss or theft caused by an employee, contractor, other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain or inflicting harm to the organization or another individual.

Real-World Scenario:
An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.

Impact:
The patient's PHI was compromised and used in an identity theft case.

Table 5 identifies vulnerabilities, impacts, and Practices to consider for accidental or intentional data loss.

Threat Quick Tips	
What to Ask?	See something? Say something! Follow your instinct, and always report what does not look or feel right to you. Beware of social engineering techniques. Check to see whether your organization conducts enhanced employee and vendor screening to make sure that those gaining access to company data are who they say they are and that they truly require access to the information. Are you limiting access to information to those who require it based on roles and responsibilities?
When to Ask?	Conduct regular security training sessions to further employees' education and awareness. Train and test your staff to make sure they understand the security risks and the consequences of falling victim to insider attack. By doing so, you can lower the probability of such attacks happening in your organization.
Who to Ask?	Always consult your IT security professionals when exposed to a situation of stolen data or employee misconduct. Every situation will vary so your IT security professionals will be able to guide you best because a cyber-threat is not limited to hacking.

What are the Threats?

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety		
Vulnerabilities	**Impact**	**Practices to Consider**
Patches not implemented promptly; includes regular and routine commercial system patches to maintain medical devices Equipment not current, or legacy equipment that is outdated and lacks current functionality Most medical devices, unlike IT equipment, cannot be monitored by an organization's intrusion detection system (IDS); safety of patients and protection of data integrity are dependent on identifying and understanding the threats and threat scenarios. However, it is the challenge of identifying and addressing vulnerabilities in medical devices that augments the risk of threats compared with managed IT products For medical devices, the cybersecurity profile information is not readily available at health care organizations, making cybersecurity optimization more challenging. This may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse effects Heterogeneity of medical devices means that the vulnerability identification and remediation process is complex and resource intensive; increases the likelihood that devices will not be assessed or patched, leading to missed opportunities to close vulnerabilities	Broad hospital operational impact due to unavailable medical devices and systems Medical devices do not function as required for patient treatment and recovery Patient safety compromised due to breach	Establish and maintain communication with medical device manufacturer's product security teams (9.L.A) Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested (9.M.B) Assess current security controls on networked medical devices (9.M.B, 9.M.E) Assess inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks (9.M.D) Implement pre-procurement security requirements for vendors (9.L.C) Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities (1.L.A) Engage information security as a stakeholder in clinical procurements (9.L.C) Use a template for contract language with medical device manufacturers and others (9.L.C) Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, MFA, and minimum necessary or least privilege (9.M.C) Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities (9.L.B) Develop and implement network security applications and practices for device networks (9.M.E)

EHNAC

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety



Description:
The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."

Real-World Scenario:
A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

Impact:
Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures.

Table 6 identifies vulnerabilities, impacts, and Practices to consider for attacks against connected medical devices.

Threat Quick Tips	
What to Ask?	Know your organization's protocols in case of a potential shutdown or attack against medical devices. Help patients and staff by understanding the processes and procedures; this can help mitigate the impacts. That means asking • How do we notify patients if their medical devices are compromised? • How do patients notify us if they suspect their medical devices are compromised?
When to Ask?	Knowledge of your organization's protocols for potential attacks on medical devices should be shared during new hire orientation or at security training. These protocols need to be communicated to patients when they are given medical devices.
Who to Ask?	Each organization should have IT security professionals to help answer any questions on the policy and governance associated with medical devices. If your organization does not, ask your supervisor for information and/or resources allowing you to learn more about the threat. Vendors or manufacturers of medical devices may need to be engaged to understand vulnerabilities, risks, and appropriate protection and response measures.

Interoperability

EHNAC

The Interoperability Factor

The Problem

What is the Problem?



TODAY - Exchange

API adoption requires point to point projects

Current adoption trajectory is slow, expensive, and at risk of significant fragmentation



FUTURE - Interoperability

A consistent infrastructure approach to API implementation

Consensus on implementation guides for key enablers, such as directory, security, patient matching, exchange and testing

DESIRED RESULT:
A national API interoperability approach that enables consistent clinical data exchange via API. We have this for administrative transactions (X12, clearinghouses, WEDI) and pharmacy transactions (NCPDP, Surescripts). We do not have this for HL7-FHIR.

The Interoperability Landscape

EHNAC

Future State

GOAL 1 — Promote Health and Wellness

- **Objective 1a:** Improve individual access to usable health information
- **Objective 1b:** Advance healthy and safe practices through health IT
- **Objective 1c:** Integrate health and human services information

GOAL 2 — Enhance the Delivery and Experience of Care

- **Objective 2a:** Leverage health IT to improve clinical practice and promote safe, high-quality care
- **Objective 2b:** Use health IT to expand access and connect patients to care
- **Objective 2c:** Foster competition, transparency, and affordability in healthcare
- **Objective 2d:** Reduce regulatory and administrative burden on providers
- **Objective 2e:** Enable efficient management of health IT resources and a nationwide workforce confidently using health IT

GOAL 3 — Build a Secure, Data-Driven Ecosystem to Accelerate Research and Innovation

- **Objective 3a:** Advance individual- and population-level transfer of health data
- **Objective 3b:** Support research and analysis using health IT and data at the individual and population levels

GOAL 4 — Connect Healthcare with Health Data

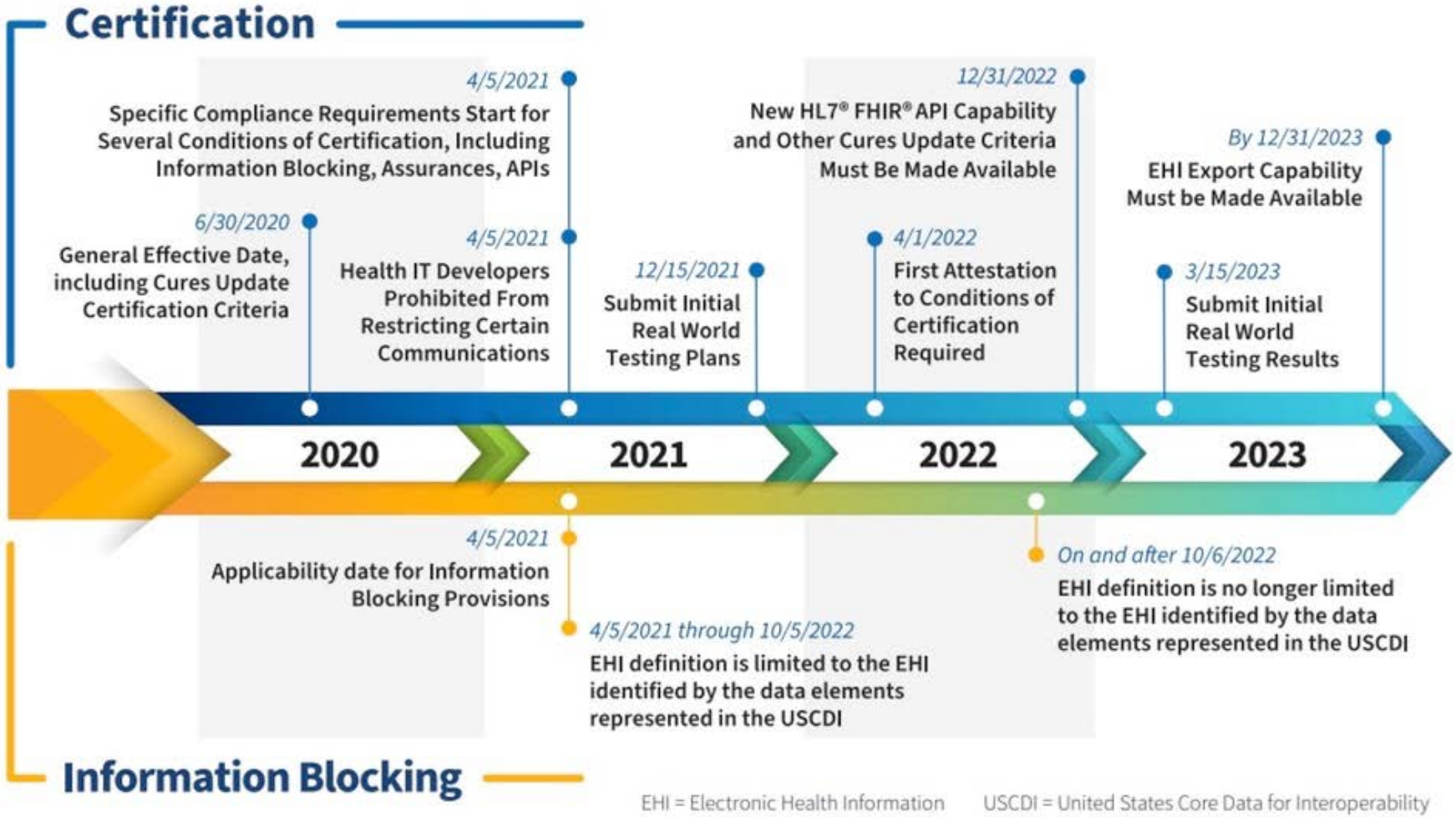
- **Objective 4a:** Advance the development and use of health IT capabilities
- **Objective 4b:** Establish expectations for data sharing
- **Objective 4c:** Enhance technology and communications infrastructure
- **Objective 4d:** Promote secure health information practices that protect individual privacy



The Office of the National Coordinator for Health Information Technology

New Applicability Dates included in ONC Interim Final Rule

Information Blocking and the ONC Health IT Certification Program:
Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency Interim Final Rule



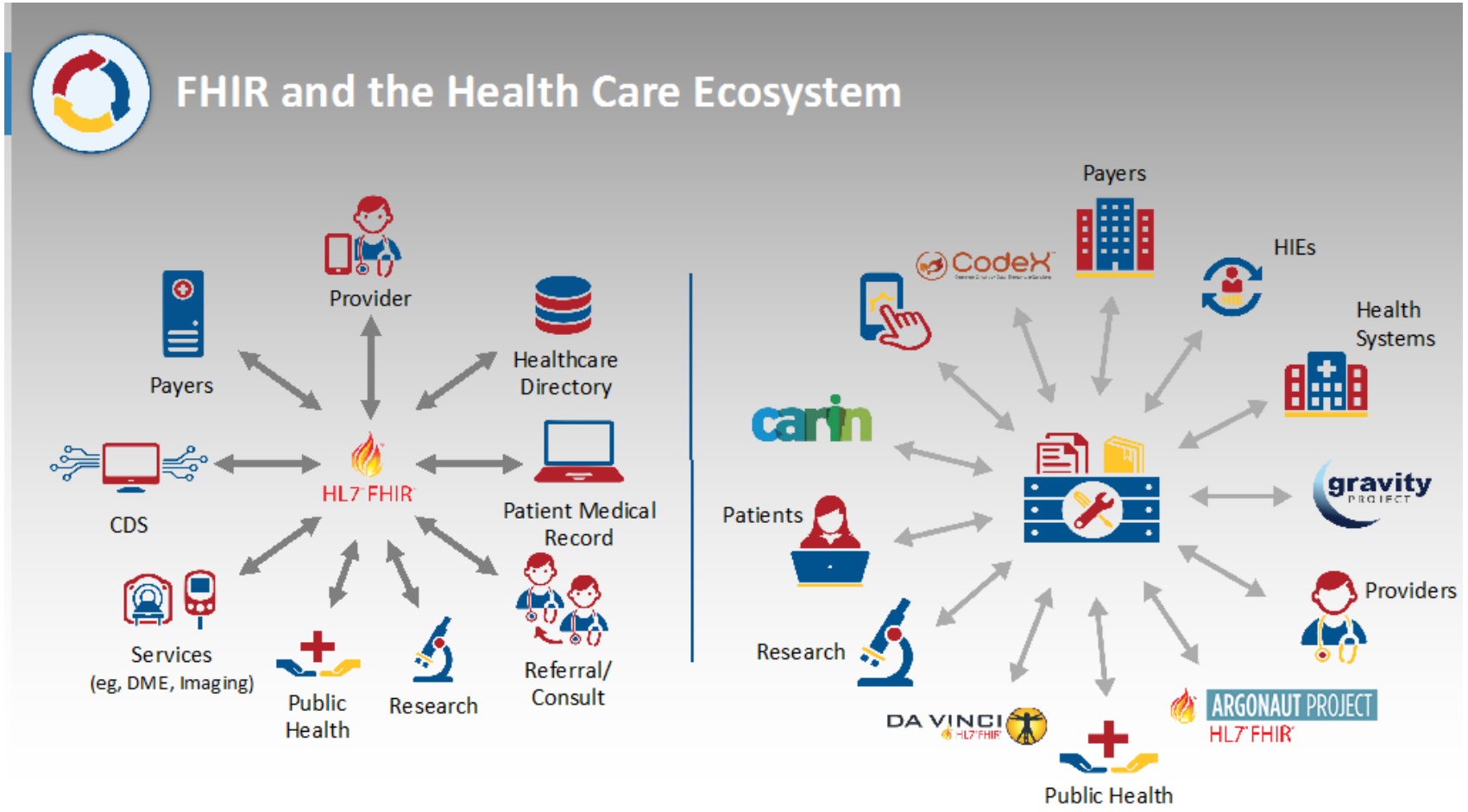
EHI = Electronic Health Information USCDI = United States Core Data for Interoperability

HealthIT.gov @ONC_HealthIT

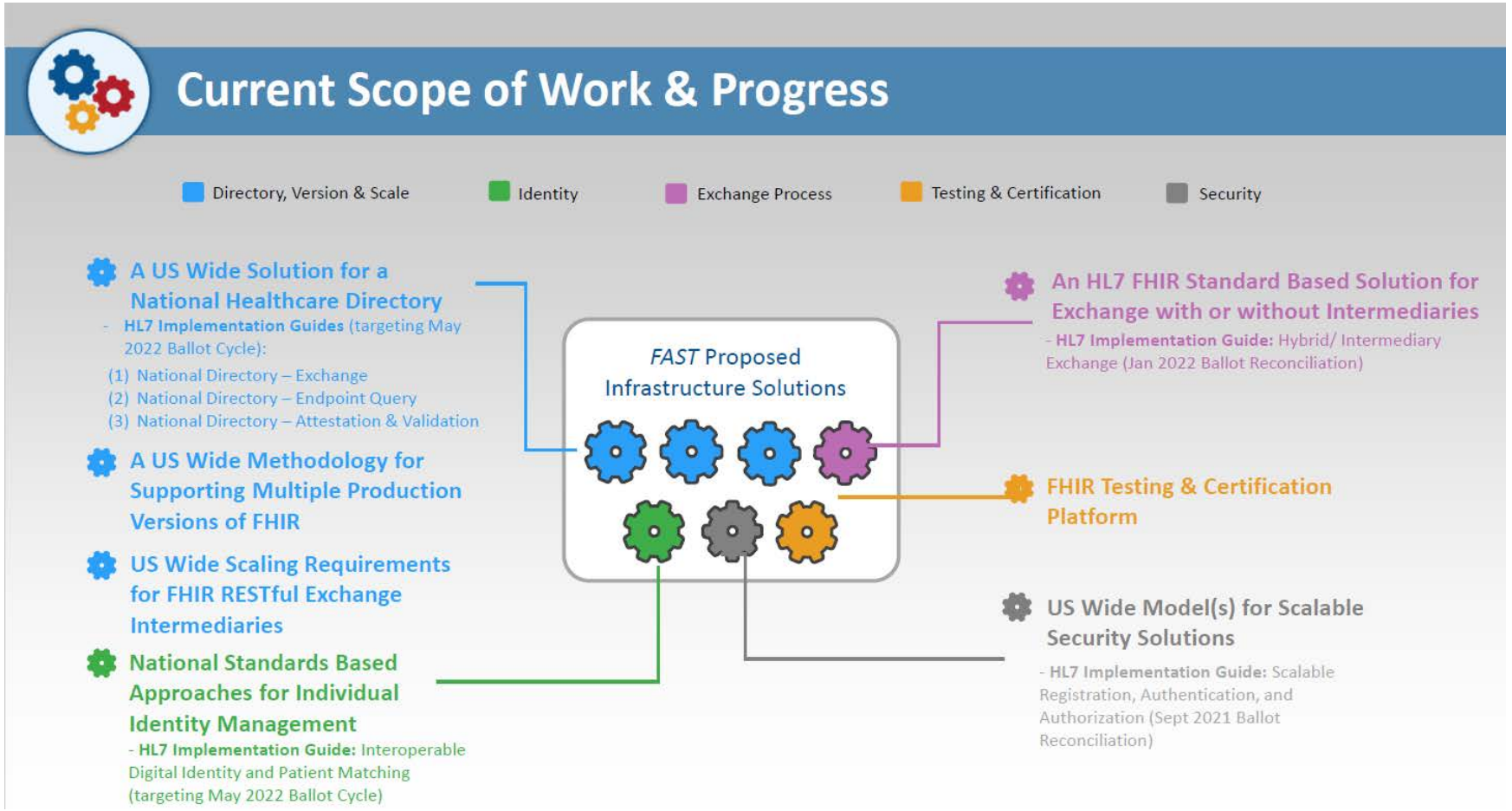
HealthIT.gov/CuresRule

The Interoperability and FHIR Factor

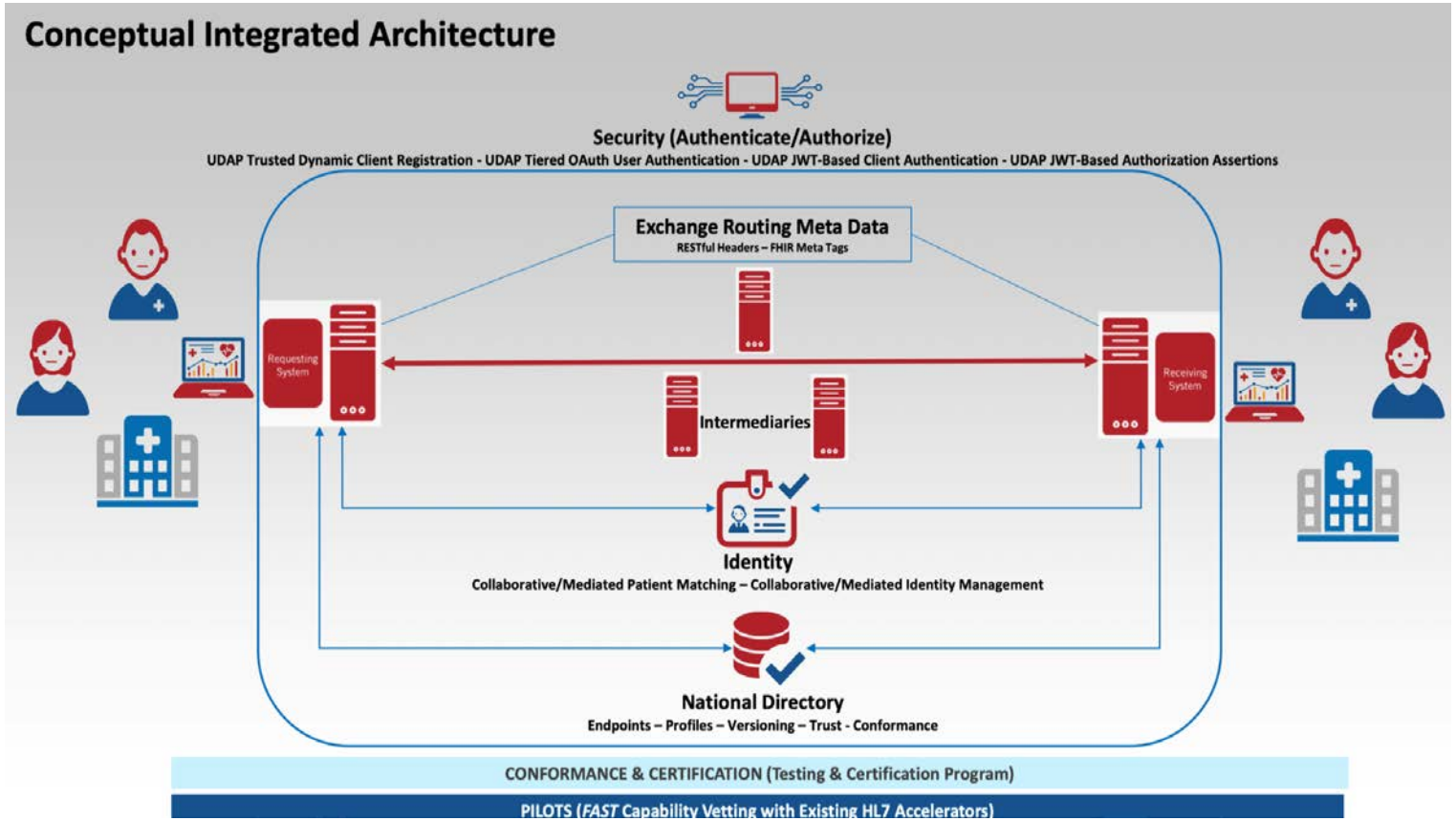
- How will we continue to advance and adopt FHIR at scale?
- Where will cross-stakeholder consensus-building take place?
  - Providers, payers, vendors and many, many others
- How will our industry handle process implications and impacts such as:
  - Recognizing new needs and changes?
  - Understanding costs and operating model impacts?
  - Advancing best practices?



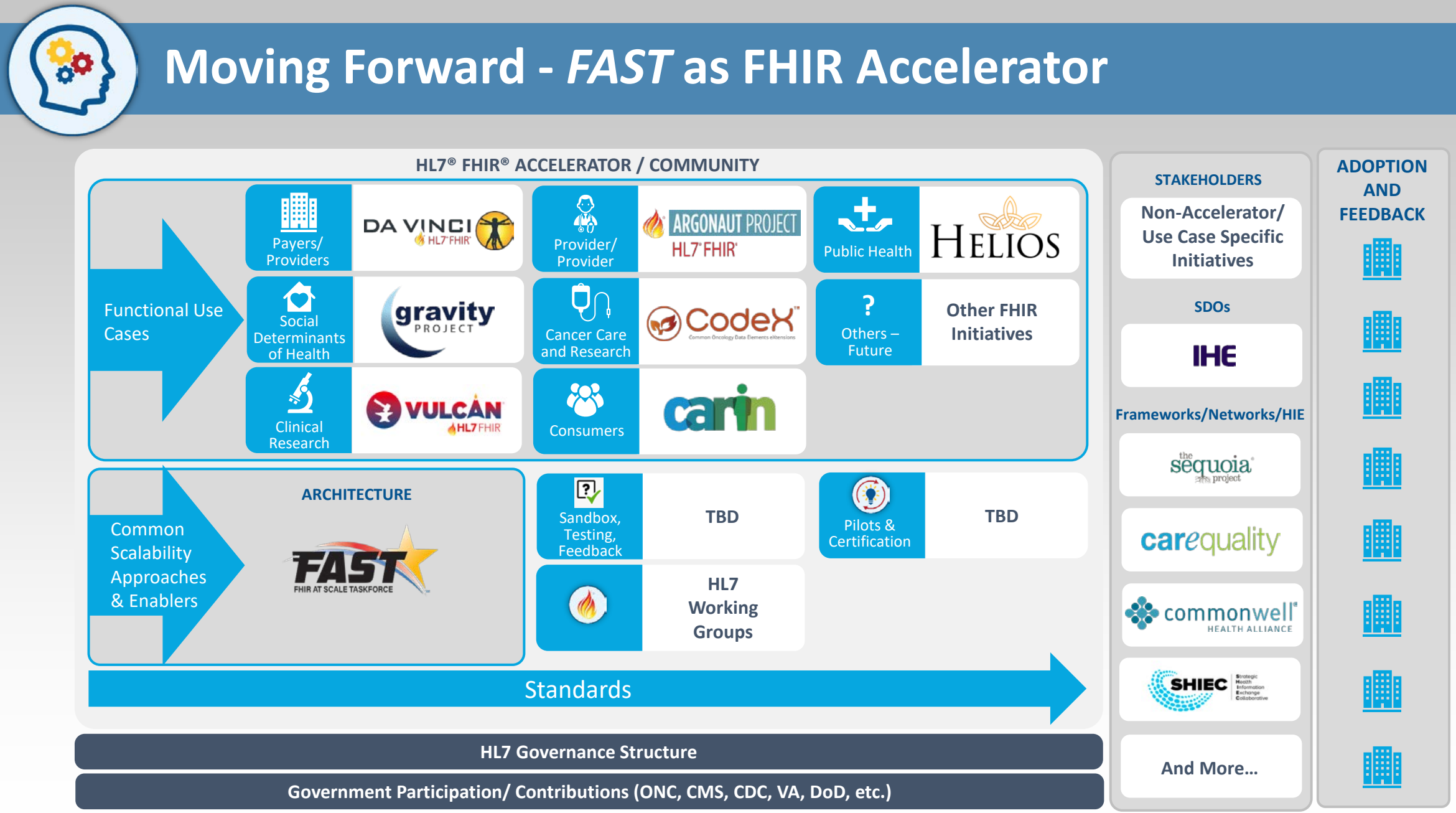
FAST Scope & Progress



ONC *FAST* Proposed Architecture



Moving Forward - *FAST* as FHIR Accelerator

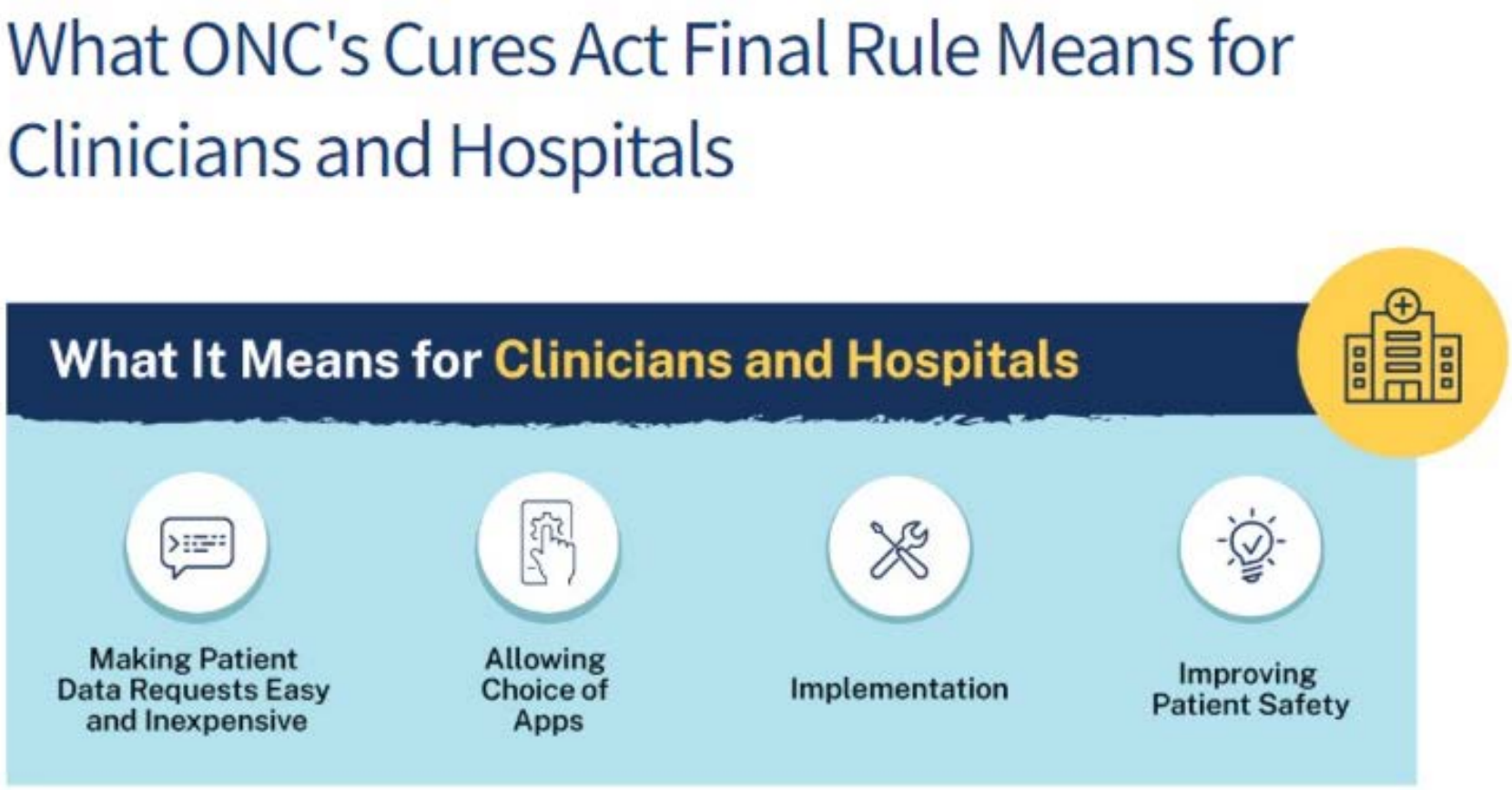


21


21st Century
Cures Act

Cures Act for Clinicians and Hospitals

EHNAC



Patient Accessibility



The Current Patient Experience

EHNAC



Access to prior medical records and imaging is critical



Complex health records and other data aren’t easily shared across systems



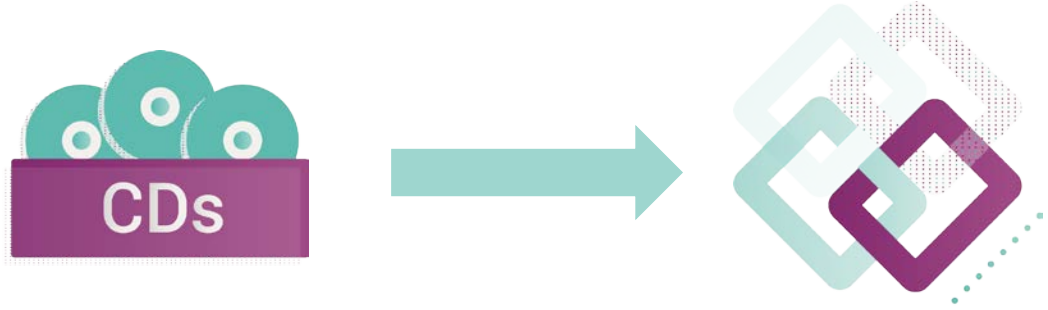
Patients typically have the burden of being courier of records during an already stressful time



The result: poor care coordination, delays in care, wasted time, anxiety, false diagnostic results, redundant testing and patient complaints

Investing in Interoperability

- Approximately 50% of images still exchanged by CD, 40% of patients receive images on CD
- Cultural resistance to change
- Economic benefits to “slow walk” efforts to unblock data
- Innovation prioritized over standardization

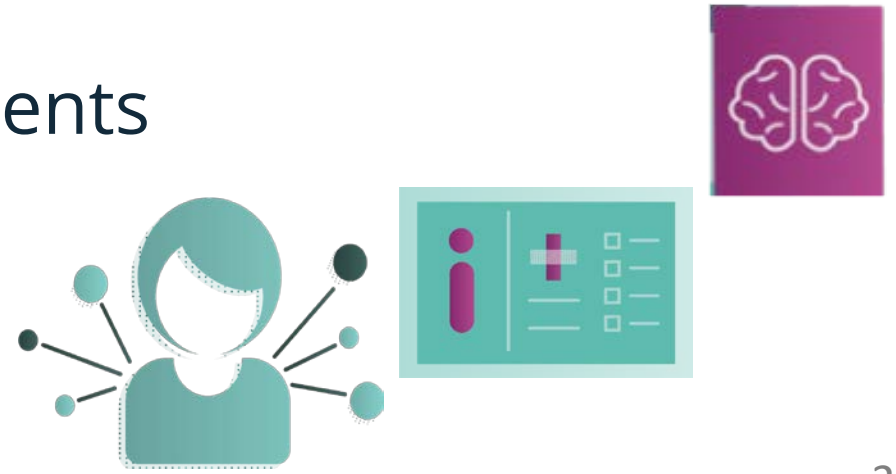


The Rise of Consumer Expectations

Patients want more influence over their own care, and demand levels of convenience they have grown accustomed to in retail, banking, travel and other industries

An accessible, easy to navigate experience is needed to meet the needs of patients spanning multiple generations and levels of digital literacy

Sharing digitally meets regulatory requirements and boosts the patient experience



The CARIN Alliance:

Identity, Authentication, and Federating Trust in the US Health Care System

Ryan Howells

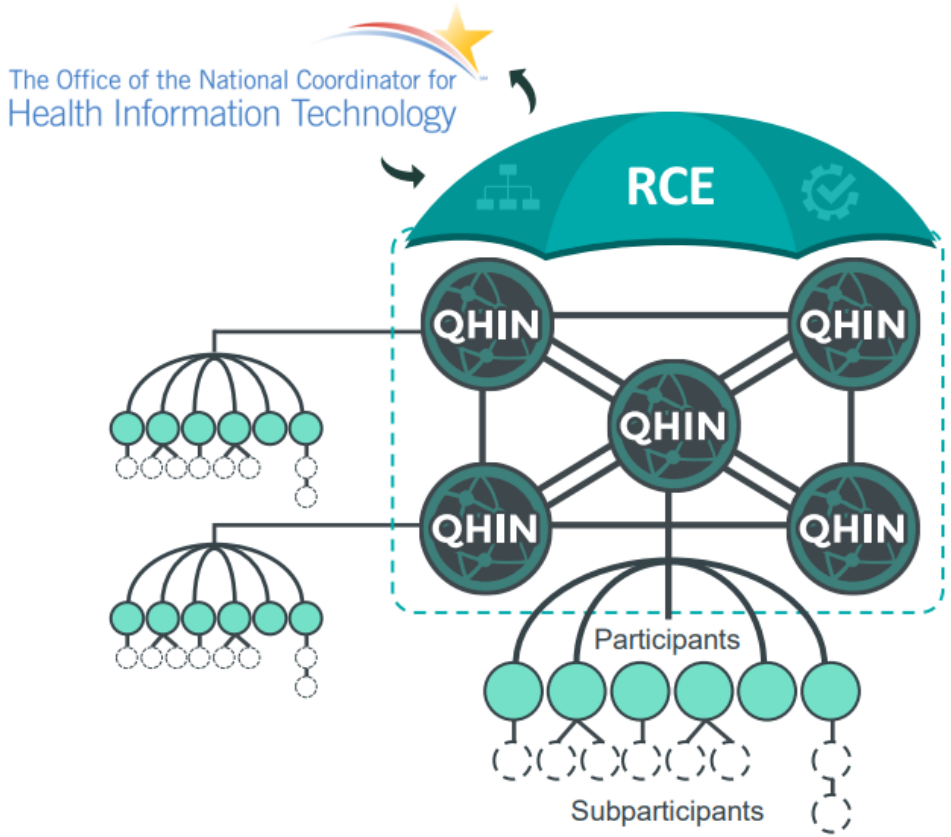
@rryanhowells | ryan.howells@leavittpartners.com

Program Manager, CARIN Alliance

@carinalliance | www.carinalliance.com

www.HL7.com/CARIN

How will exchange work under TEFCA?



ONC defines overall policy and certain governance requirements.

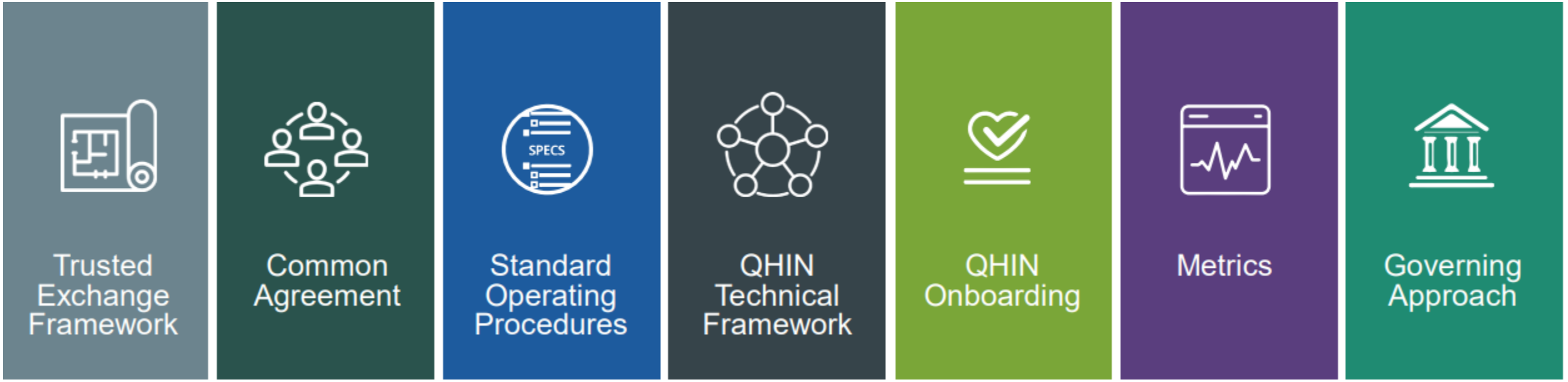
RCE provides oversight and governing approach for QHINs.

Qualified Health Information Networks (QHINs) connect directly to each other to facilitate nationwide interoperability.

Each QHIN connects Participants, which connect Subparticipants.

TEFCA Components

EHNAC



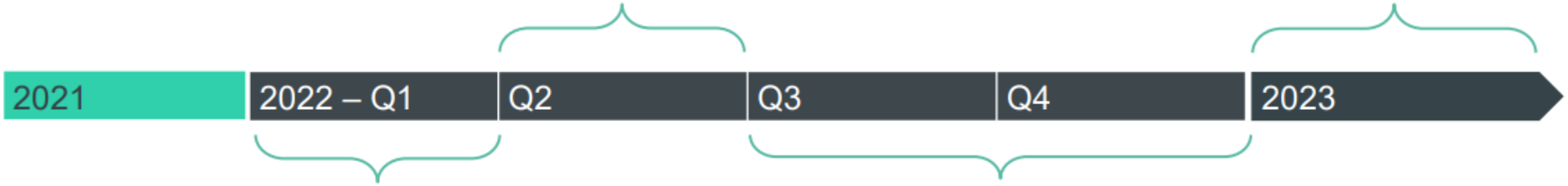
Timeline to Operationalize TEFCA

EHNAC

2021
- Public engagement
- Common Agreement Work Group sessions
- RCE and ONC use feedback to finalize TEFCA

Q2 of 2022
- QHINs begin signing Common Agreement and applying for designation

2023
- Establish Governing Council
- Follow change management process to iterate Common Agreement, SOPs, and QTF, including to support FHIR-based exchange



Q1 of 2022
- Publish Common Agreement Version 1
- Publish QHIN Technical Framework (QTF) Version 1 and FHIR Roadmap
- Initiate work to enable FHIR-based exchange
- Public education and engagement

Q3 and Q4 of 2022
- Onboarding of initial QHINs
- Additional QHIN applications processed
- RCE establishes Transitional Council
- RCE begins designating QHINs to share data
- Prepare for TEFCA FHIR exchange pilots

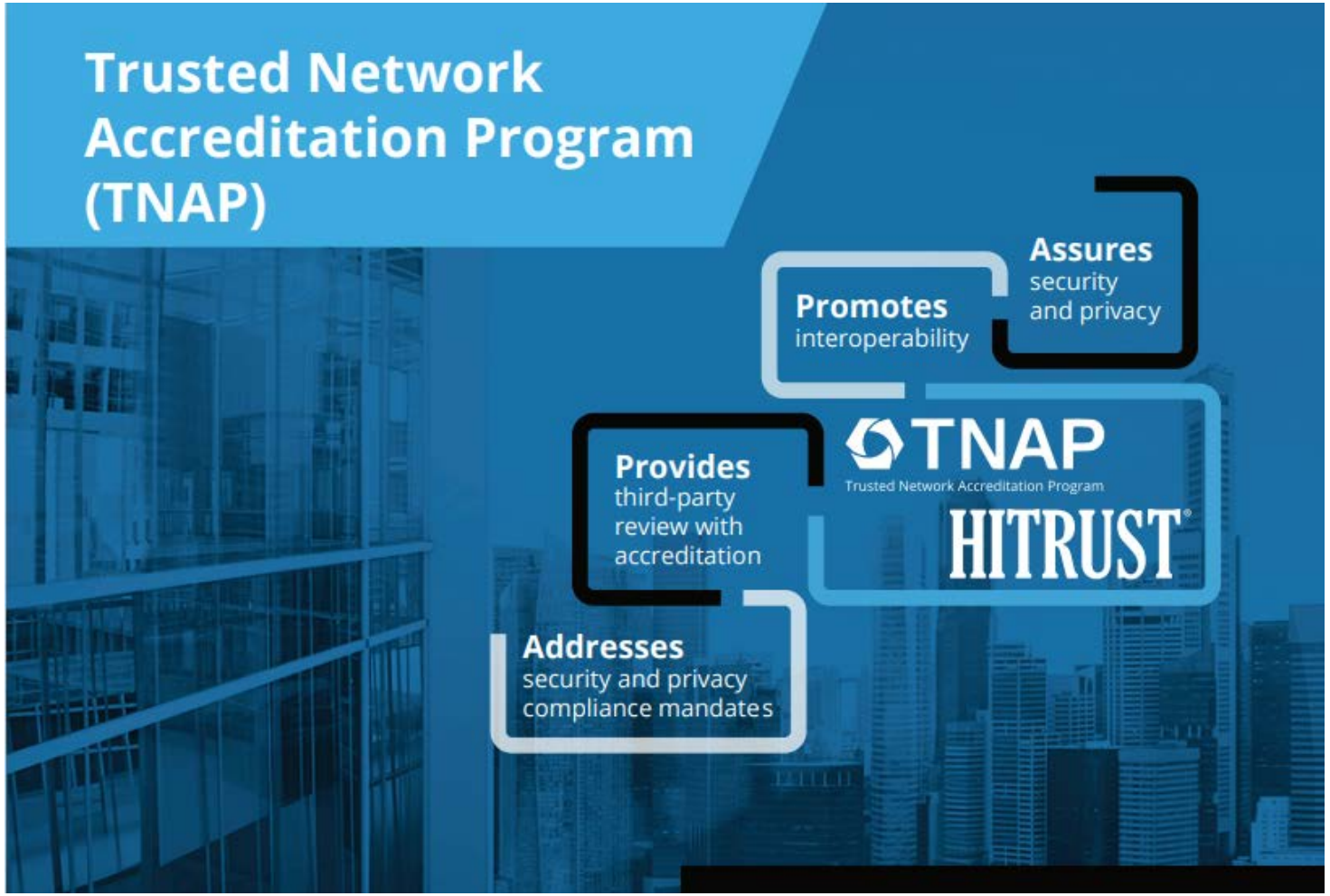
Options

EHNAC

Some Potential Options for Consideration

Trusted Network Accreditation Program (TNAP)

EHNAC



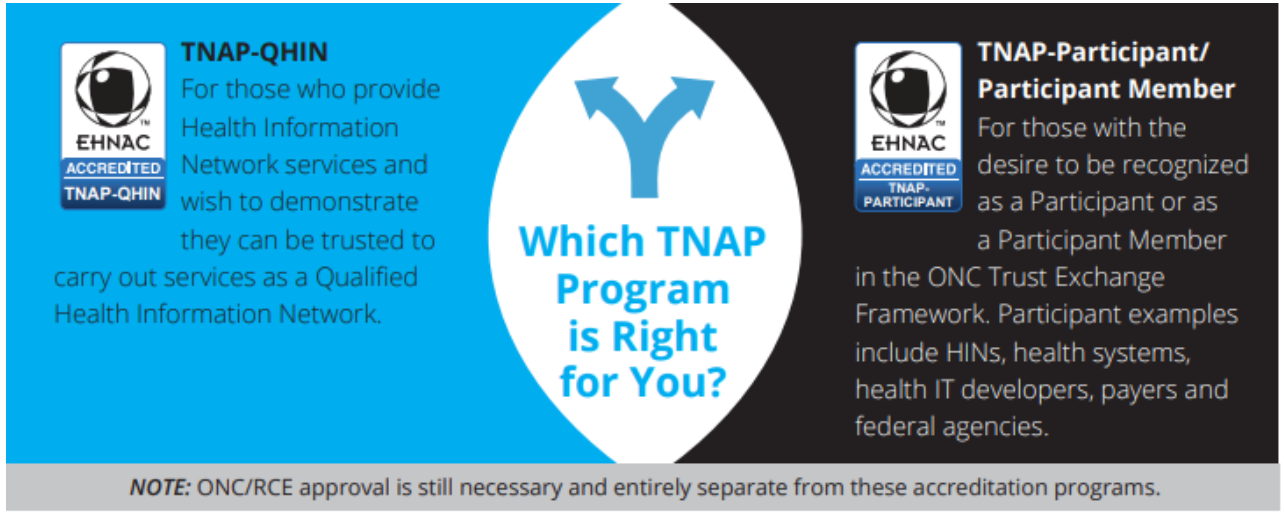
The Programs

EHNAC

Promoting Interoperability and Assuring Security & Privacy

TNAP
Trusted Network Accreditation Program

HITRUST



Trust Is Everything in Healthcare

TNAP-QHIN and TNAP-Participant candidates must hold HITRUST CSF Validated Assessment with Certification

info@trustednetworkap.org
860-408-1620
trustednetworkap.org



What Should Your Organization be Considering for Next Steps?

Your Cyber Hygiene Scorecard

Annual Risk Assessment
Annual Asset Inventory
Assure Timely Software Patches and Software Updates
Assure Every 4 mo. Password Changes
Multi-Factor Authentication (MFA)
Assure Minimum Backup Regimen
Assure Minimum Annual Staff Training
Have a Documented Contingency Plan
Test Contingency Plan and revise as appropriate
Cyber Insurance

Resources

EHNAC

New 405(d) Cybersecurity Resource



How to Implement Data Security

A security breach is the **loss** or **exposure** of sensitive data, including information relevant to the organization's business and patient **Protected Health Information (PHI)**. Impacts to the organization can be profound if data files are corrupted, lost, or stolen. Thus, good data security practices **protect your organization and your patients.**

Why is it important? When security breaches of data occur, it can prevent your employees from completing work accurately or on time and could result in potentially devastating consequences to your patients' medical treatment and wellbeing. Secure organizational data is not only important for your patients, but also for your organization's financial wellbeing and reputation.

Not sure where to start? We've got you covered! We have created three "How-to" resources-one for small, one for medium, and one for large organizations so that you can start protecting your patients from cyber threats right now!

Download the Resources Below!

Small Organizations
Medium Organizations
Large Organization

For more information and resources visit our website at 405d.hhs.gov!

Contact Information

Lee Barrett, EHNAC
lbarrett@ehnac.org

