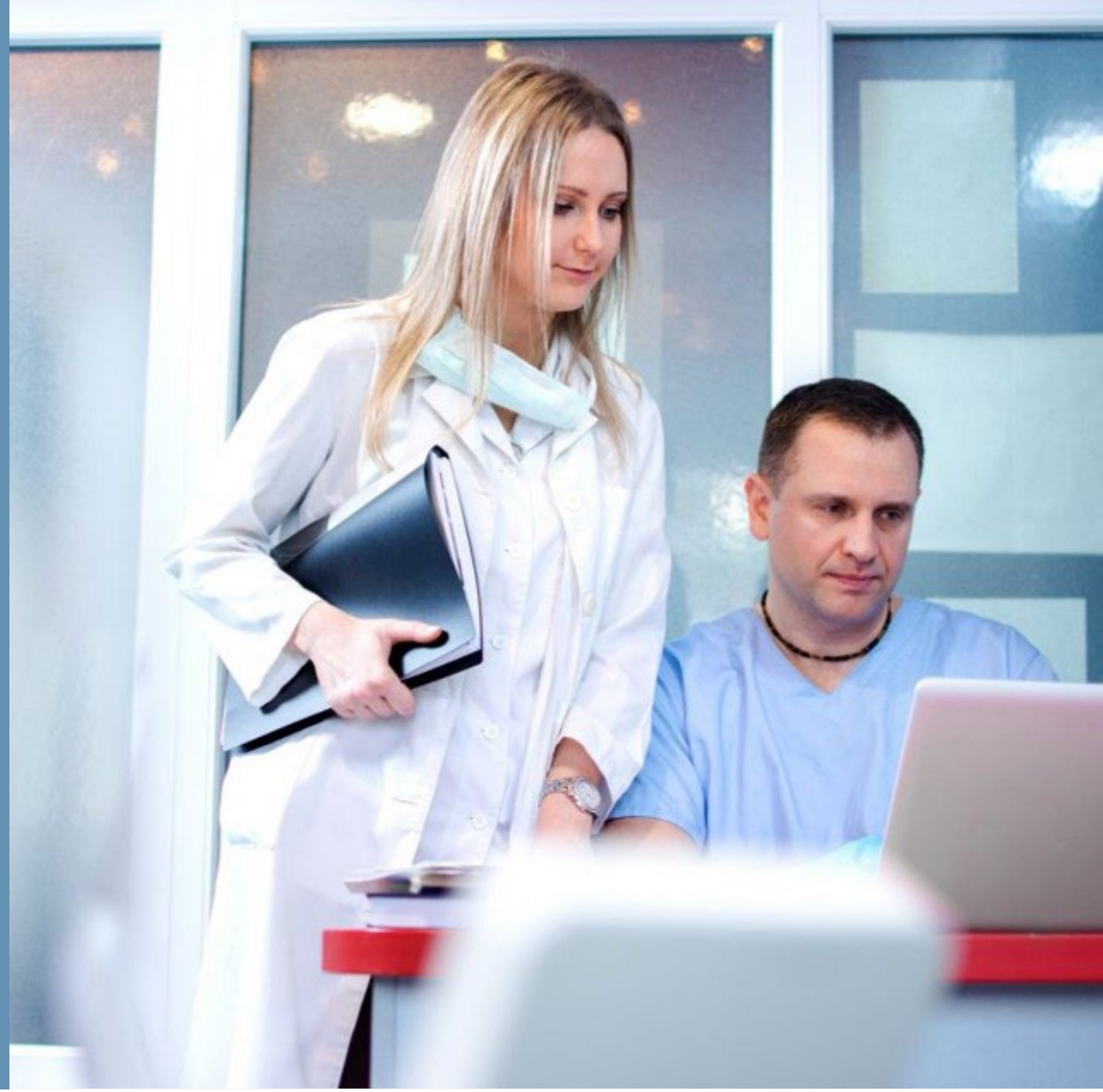
Preparing Health Systems to Mitigate Cyber Threats/Introduction to HITRUST

November 10, 2022



mazars

1. A Data Breach Should be Expected ☹
2. Can you Trust your Vendors to secure PHI? ☹
3. Protecting a Health System's Information Assets – HIPAA Risk Assessment ☺
4. Protecting the Health System's Information Assets – HITRUST Assessment ☺
    - Becoming HITRUST Certified
    - Basic, Current-state (bC)
    - Implemented, One-Year
    - Risk-based, Two-Year
4. Questions/Discussion

01

A Data breach should be expected

Safeguarding protected health information

Healthcare is an attractive target

- Value of personal health data, ranging from $10 to $1,000 per record in online marketplaces, depending on completeness (=> high rate of return)
- Fairly continuous stream of new employees (-> many new targets)
- Interconnected systems (-> broad and fertile attack surface)
- Vendor products with varying levels of safeguards (-> easy entry points)
- Lack of security resources and processes (-> relatively weak defenses)
- Criticality of services provided (-> susceptible to extortion)

Safeguarding protected health information

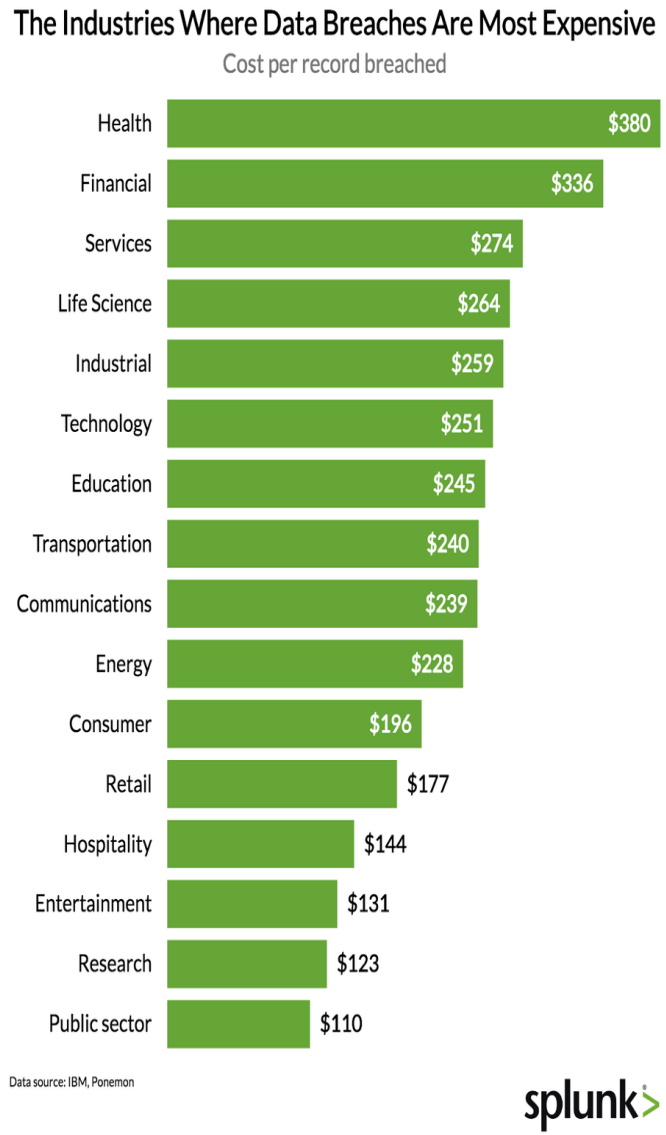
Threat landscape is continuously evolving

- Reportedly, 50% of US firms were breached by ransomware last year
- Nearly 35% of these firms paid the ransom to release their data
- However, only about 70% of those victims who paid regained access to their data
- Ransomware has evolved into a “double extortion” – attackers extract sensitive information (sometimes for months) before encrypting files
- If the victim hesitates to pay, the hackers release some of the stolen data and threaten to post the remainder

Safeguarding protected health information

Healthcare provides a large attack surface for criminals to exploit

- In general, there are four (4) key paths for exploitation: stolen credentials, phishing attacks, exploited vulnerabilities & use of botnets.
- Ransomware has continued its upward trend, involved in approximately 25% of total breaches this past year.
- Supply chain was responsible for 62% of system intrusion incidents in 2021. The healthcare industry was the most common victim of attacks caused by third parties, accounting for 33% of incidents in 2021.
- 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing or simply due to an error, people continue to play a very large role in incidents and breaches alike.



02

Can you trust your vendors to secure PHI?

Can you trust your vendors to secure PHI?

- Healthcare organizations outsource numerous processes and services, but they remain legally accountable for the safeguarding of their patients' data (PHI).
- Your vendors' ineffective policies and procedures can lead to significant fines and penalties from OCR; however, reputational loss and other additional costs can be significantly more impactful.
- Continual monitoring of security-related Service Level Agreements (SLAs) and requiring external audits (e.g., SOC2, HITRUST) are the most effective means to gain assurance of the cyber protection of your data held by third parties.

Common privacy rule violations

- Extended amount of time to provide patient data
- Impermissible disclosure of PHI
- Lack of / noncompliant BAAs

Common security rule violations

- Failure to conduct an enterprise-wide risk analysis
- Poor risk management processes
- Ineffective access controls

Can you trust your vendors to secure PHI?

Verify that your vendors can provide assurances that they fully comply with HIPAA regulations and industry best practices for safeguarding of PHI.

- Conduct third-party screening, onboarding & due diligence
- Build mature third-party risk management (TPRM) processes
- Clearly define roles, responsibilities, escalation paths, obligations, timeframes
- Ensure security service level agreements (SLAs) exist in contracts
- Require annual external audits of critical third parties

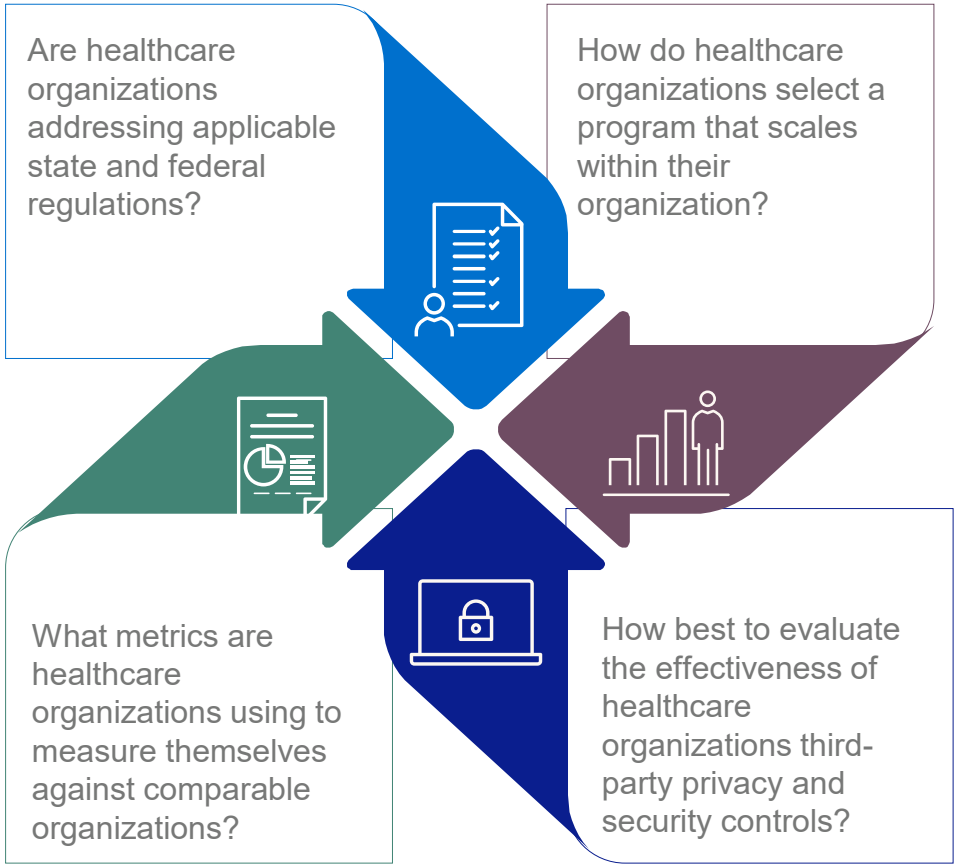
03

Protecting the Heath System's Information Assets

Risk Assessment

Protecting the HCO's Information Assets
HIPAA Risk Assessment

Healthcare organizations need a comprehensive information risk management and compliance program



Protecting the HCO's Information Assets
HIPAA Risk Assessment

What is a risk assessment?

- A comprehensive look at the organization's security posture that aims to uncover potential threats and vulnerabilities within the IT ecosystem
- Sometimes known as a security assessment or risk analysis
- Can assure the confidentiality, integrity and availability of electronic PHI held by the organization

Items for consideration

- Serves as a critical factor in assessing whether an implementation specification is reasonable and appropriate
- Can do more than just help organizations stay compliant with HIPAA; they can help address possible vulnerabilities above and beyond the regulations
- Regular (i.e., at least annual) risk assessments are essential and necessary

Protecting the HCO's Information Assets
HIPAA Risk Assessment

What is a risk assessment?

HHS requires that the seven (7) elements of a risk analysis must be incorporated into the assessment:

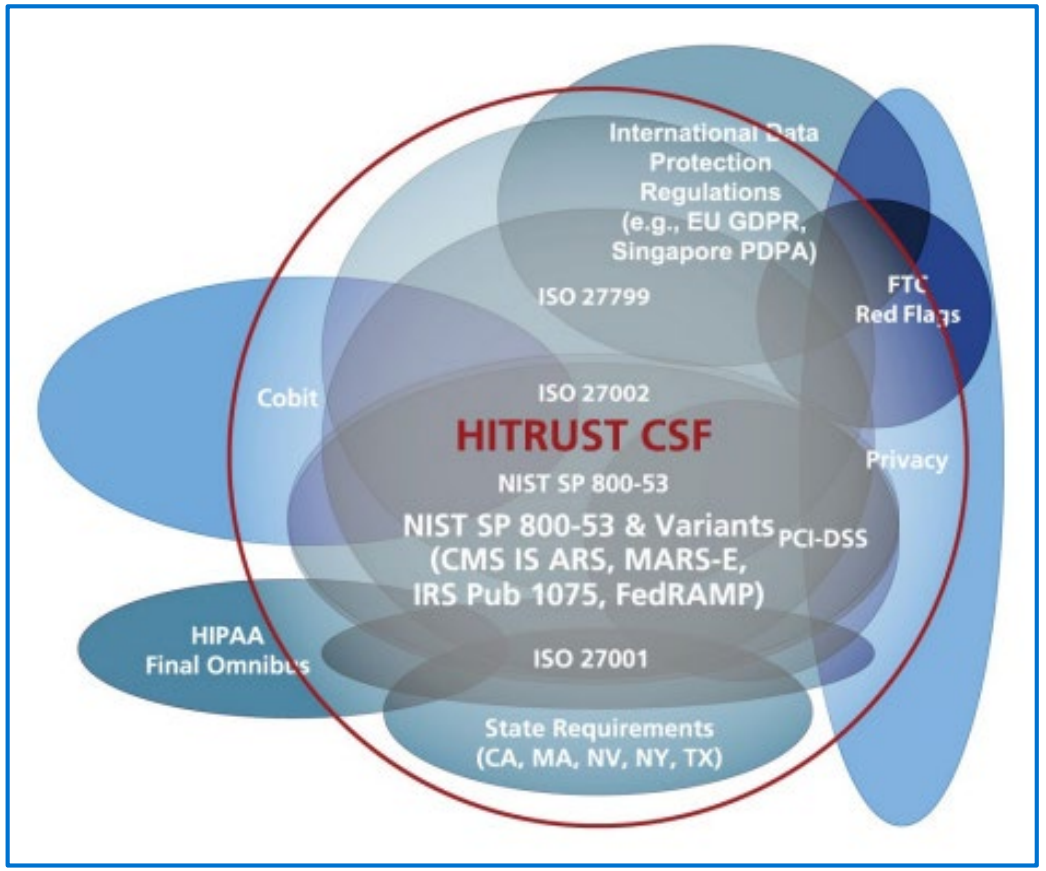
1. Determine scope
2. Collect data
3. Identify threats and vulnerabilities
4. Assess likelihood of threat
5. Assess level of risk
6. Document
7. Monitor and update

04

Protecting the Health System's Information Assets
HITRUST Assessments

Protecting the HCO's Information Assets
Becoming HITRUST certified

- **Reduced risk** – Provides a clear understanding of your data integrity posture so that you can address any weaknesses and reduce your risk now and into the future
- **Competitive advantage** – Being able to assure your stakeholders that their data is protected and valuable in a digital world
- **Industry-leading benchmarking** – As the industry-leading standard for data security, HITRUST ensures that you are using best practices and achieving compliance across a full spectrum of regulatory and professional standards
- **Enhanced partnership opportunities** – Many companies are required to ensure their third-party vendors have robust data security programs in place
- **Trust** - HITRUST is the most streamlined, trusted way that you can let your stakeholders know that you take data security seriously.



Source: HITRUST

Protecting the HCO's Information Assets
Becoming HITRUST certified

HITRUST – Growing Compliance Objective for Healthcare Organizations & Vendors

HITRUST was created by a consortium of nine healthcare organization to address:

(1) Concern over data breaches

(2) Inconsistent requirements and standards for safeguarding data

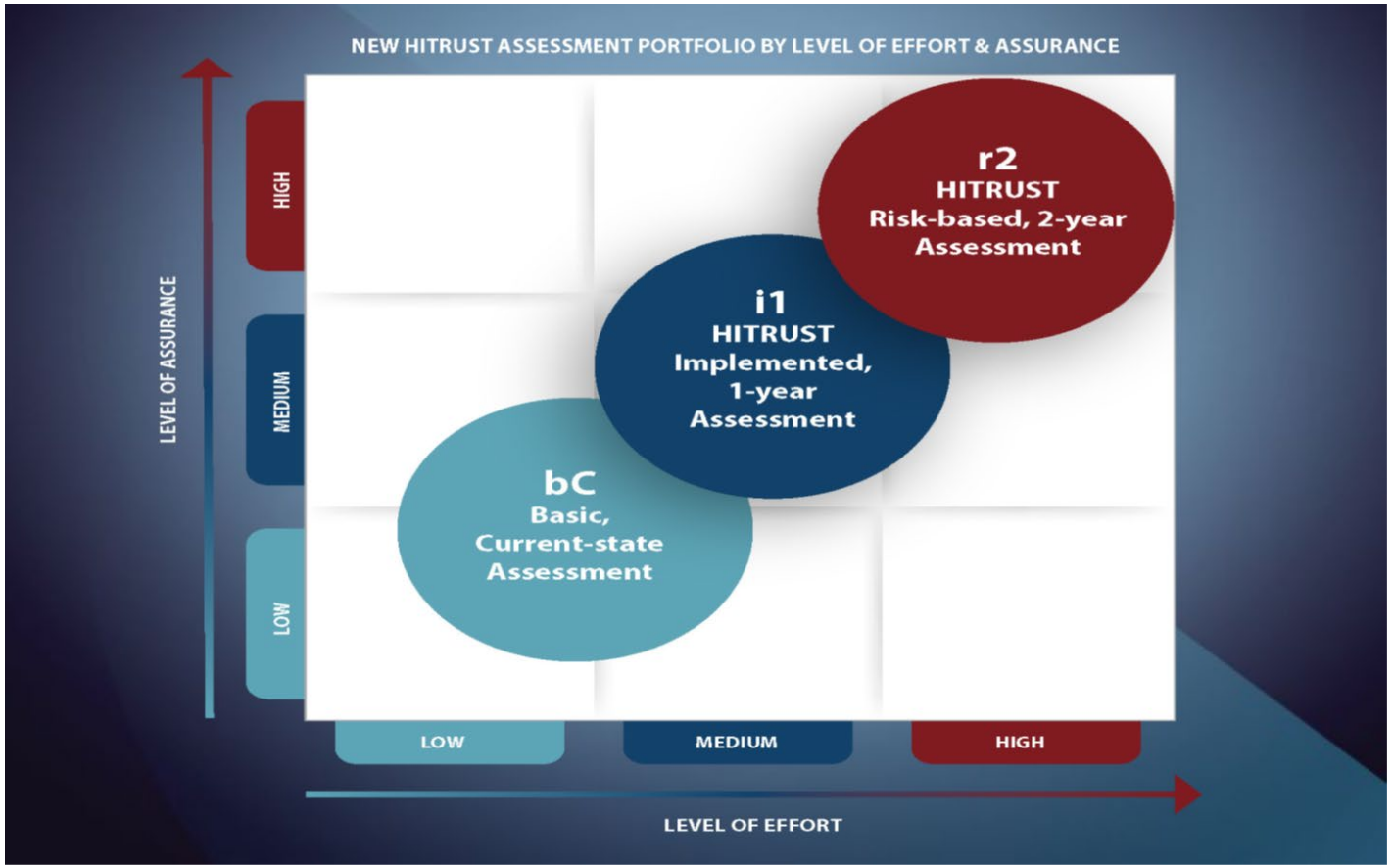
(3) Compliance issues

(4) The growing risk and liability associated with information security in the healthcare industry

All organizations that intend to contract with a consortium member must be HITRUST certified.

Protecting the HCO's Information Assets
Becoming HITRUST certified

HITRUST Assessment Types:



Source: HITRUST

Protecting the HCO's Information Assets
HITRUST Basic, Current-State (bC) Assessment

Verified self-assessment focused on good information security hygiene

- A relatively fast, low-effort approach for evaluating the current status of your information protection program or providing basic assurances for your stakeholders
- Uses the HITRUST CSF framework, which harmonizes multiple authoritative sources and provides prescriptive control requirements
- Offers ability to tailor the assessment to include only specific, needed control requirements
- Assessment information is "verified" by the HITRUST Assurance Intelligence Engine to provide a level of quality assurance review
- Includes 71 control requirement statements, targeted to NISTIR 7621 standards (Small Business Information Security Fundamentals)
- Serves as a starting point for the more rigorous i1 and r2 HITRUST assessments – all 71 bC requirements are included in an i1
- Can also serve as an effective means to obtain good security hygiene assurances from vendors that don't process/store a significant volume of sensitive data

Protecting the HCO's Information Assets
HITRUST Implemented, One-Year (i1) Assessment

Leverages security best practices and current threat intelligence to defend against cyberthreats

- A "best practices" assessment recommended for moderate risk situations
- Designed to keep pace with the latest cyberattack threats, via a threat-adaptive control set that evolves over time to deliver continuous cyber relevance
- Addresses gaps found in other cybersecurity frameworks, such as:
  - Required controls not always current or relevant
  - Emerging cybersecurity risks not always addressed
  - Low frequency of updates
  - Lack of prescriptiveness
- Focuses on implementation to assure that control requirements are operating as intended
- Substantially covers the following authoritative sources: NIST SP 800-171, HIPAA Security Rule (95%), GLBA Safeguards Rule, EBSA Cybersecurity Best Practices, Health Industry Cybersecurity Practices (HICP)
- One-year certification can help justify reductions in cyber insurance premiums
- HCOs can begin with an i1 and migrate to an r2 over time

Protecting the HCO's Information Assets
HITRUST Implemented, One-Year (i1) Assessment

The provider third-party risk management council (ptprm) assurance guidance

- PTPRM comprised of prominent Chief Information Security Officers (CISOs) from leading health systems and provider organizations
- Recommends and promotes best practices to effectively manage information security-related risks in HCO supply chains and to safeguard patient information
- Requires their moderate risk vendors to provide information security **assurances through a HITRUST i1 certification,** rather than providing other assurance mechanisms (e.g., SOC2)
- Encourages HCOs to join to protect patient data, reduce administrative costs of proprietary TPRM programs and reduce burden on vendors via standardized assurance mechanisms

It's critical for HCOs to show that their PHI is protected, and that information security is a top priority.

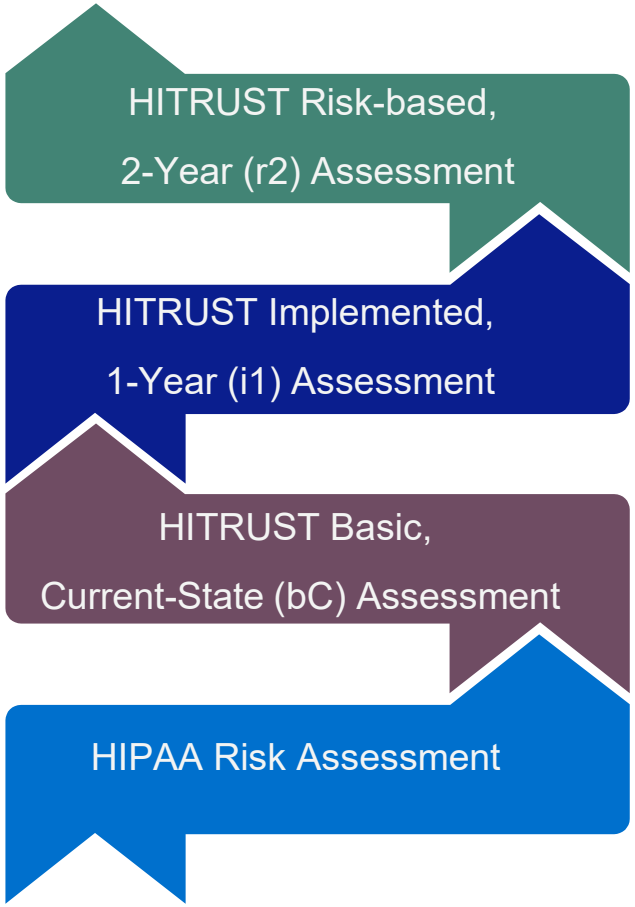
Allegheny Health Network
Cleveland Clinic
UPMC LIFE CHANGING MEDICINE
VANDERBILT UNIVERSITY MEDICAL CENTER
University of Rochester
wellforce Tufts Medical Center
Mayo Clinic

Protecting the HCO's Information Assets
HITRUST Risk-based, Two-Year (r2) Assessment

Gold standard for providing highest level of information protection and compliance assurance

- Provides recognition that the organization meets and exceeds industry-accepted information security requirements.
- Comprehensiveness of control requirements, depth of quality review and consistency of oversight.
- Offers flexible, able-to-be-tailored, risk-based control selection to meet the most stringent needs.
- Relies on quantitative measurements to accurately evaluate, score and assess the maturity of an organization's information risk management program.
- Organizations can select whichever risk factors and compliance factors they require, including:
  - NIST CSF
  - SP 800-53
  - ISO 27001
  - FedRAMP
  - FISMA
  - HIPAA
  - FTC
  - Red Flags Rule
  - MARS-E
  - PCI DSS
  - CCPA
  - GDPR
  - AICPA Trust Services Criteria
  - Plus 30+ other industry-recognized standards and authoritative sources
- The r2 Certification is valid for two years.

Protecting the HCO's Information Assets
HITRUST Roadmap



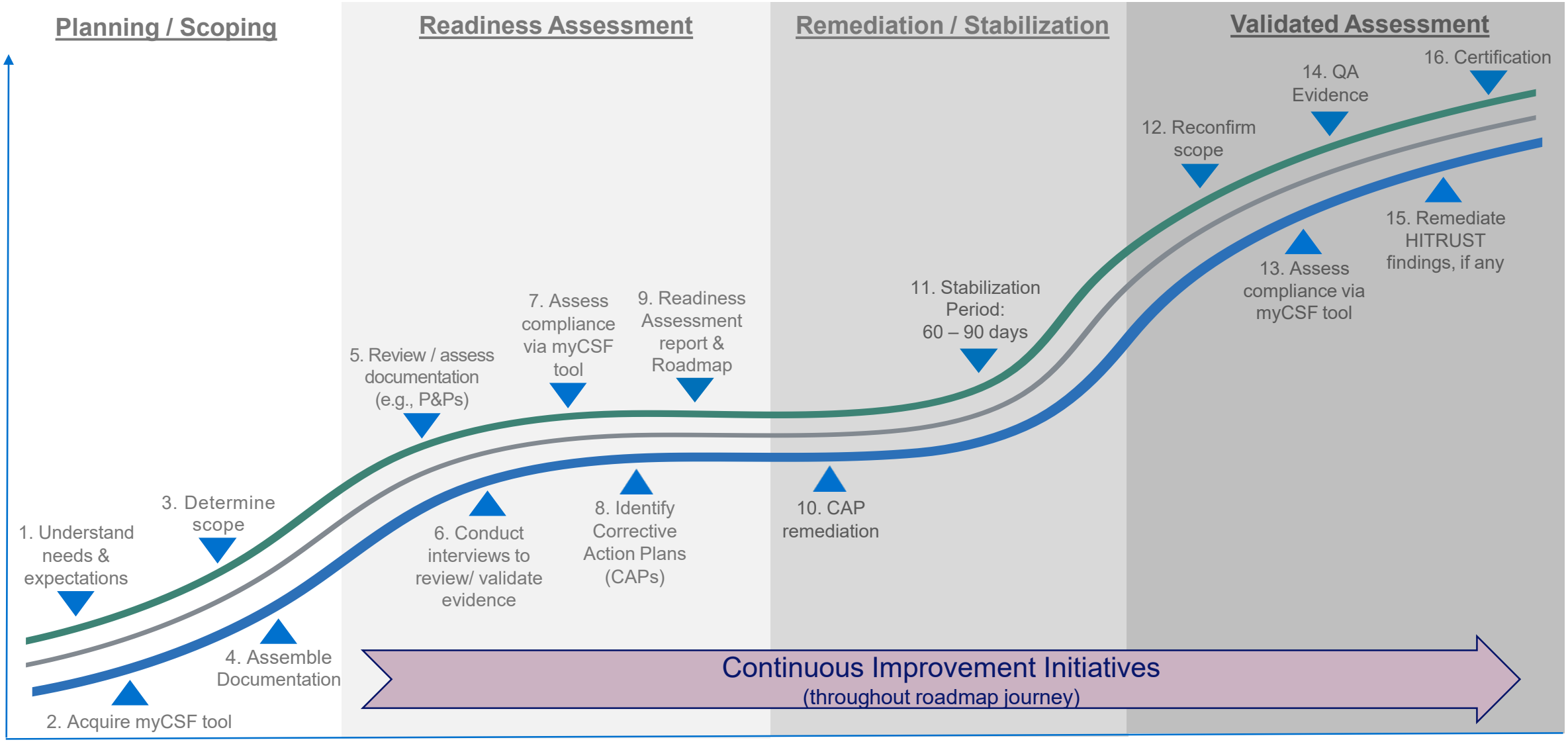
- Gold standard
- Highest level of assurance

- Leverages security best practices
- Threat-adaptive control set

- Focused on good information security hygiene
- Serves as a starting point for either an i1 or r1

- An essential, first step to keep PHI safe and avoid penalties for violations

The Journey to HITRUST Validation Assessment



Typical elapsed time: 12 – 18 months

Why Should Clients Pursue HITRUST Certification Over Risk Assessment?

HITRUST focuses on continuously developing tools, products and services that improve information risk management and compliance, doing the heavy lifting so that you can focus on the real task at hand: Driving your business.

05

Questions/Discussion

Contact

Mazars

Justin Frazer, Director
Healthcare Consulting Practice
justin.frazer@mazarsusa.com

William Ahrens, Director
Healthcare Consulting Practice
william.ahrens@mazarsusa.com

About Mazars

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of more than 44,000 professionals – 28,000+ in Mazars' integrated partnership and 16,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*Where permitted under applicable country laws

Mazars USA LLP

Mazars USA LLP is an independent member firm of Mazars Group, an international audit, tax and advisory organization with operations in over 90 countries. With roots going back to 1921 in the US, the firm has significant national presence in strategic geographies, providing seamless access to 28,000+ professionals around the world. Our industry specialists deliver tailored services to a wide range of clients across sectors, including individuals, high-growth emerging companies, privately-owned businesses and large enterprises.

www.mazars.us

Follow us:

LinkedIn:
www.linkedin.com/company/mazarsinus

Twitter:
www.twitter.com/mazarsinus

Facebook:
www.facebook.com/mazarsinus

mazars