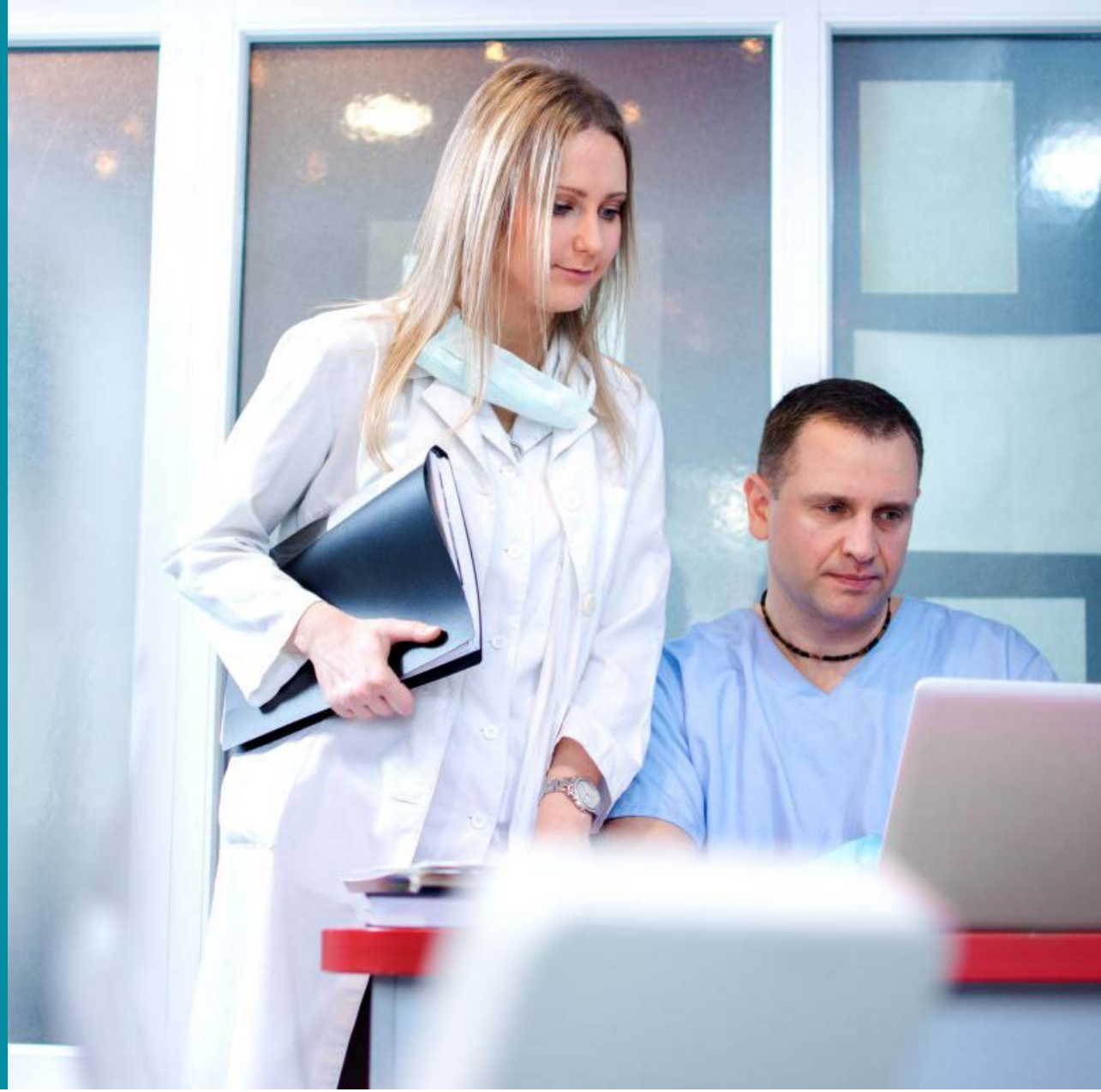
# Tools and methods to assure HIPAA compliance

June 2022



mazars

# Agenda

1. Safeguard protected health information
2. Protecting business – risk assessment
3. Protecting business – HITRUST
4. Final thoughts

01

Safeguard protected health information

**PHI**

# Safeguard protected health information
# **PHI**

## Healthcare's need to protect PHI

- Need to comply with federal, state and other regulations (e.g., HIPAA, CMS, PCI-DSS, CCPA, GDPR)
- Limited staff, skills, and expertise to provide data privacy and security assurances
- Increased use of cloud-based applications resulting in increased concerns of data privacy / security breaches
- Poor existing cybersecurity practices and potential for ransomware attacks
- Board and Executive Management concerns over daily news reports of malware attacks and breaches affecting health care organizations

# Safeguard protected health information
# **PHI**

## Healthcare is an attractive target

- Value of personal health data, ranging from $10 to $1000 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 low defenses)
- Criticality of services provided (-> susceptible to extortion)

# Safeguard protected health information
# **PHI**

## 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

# Safeguard protected health information
# PHI

## Healthcare provides a large attack surface for criminals to exploit

- In general, there are 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
    - Elekta (42 health systems)
    - LogicGate (47K patient records)
- 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.
    - For example, misconfiguring of cloud storage environments accounts for a significant percentage of breaches due to human error

**Verizon 2022 DBIR**

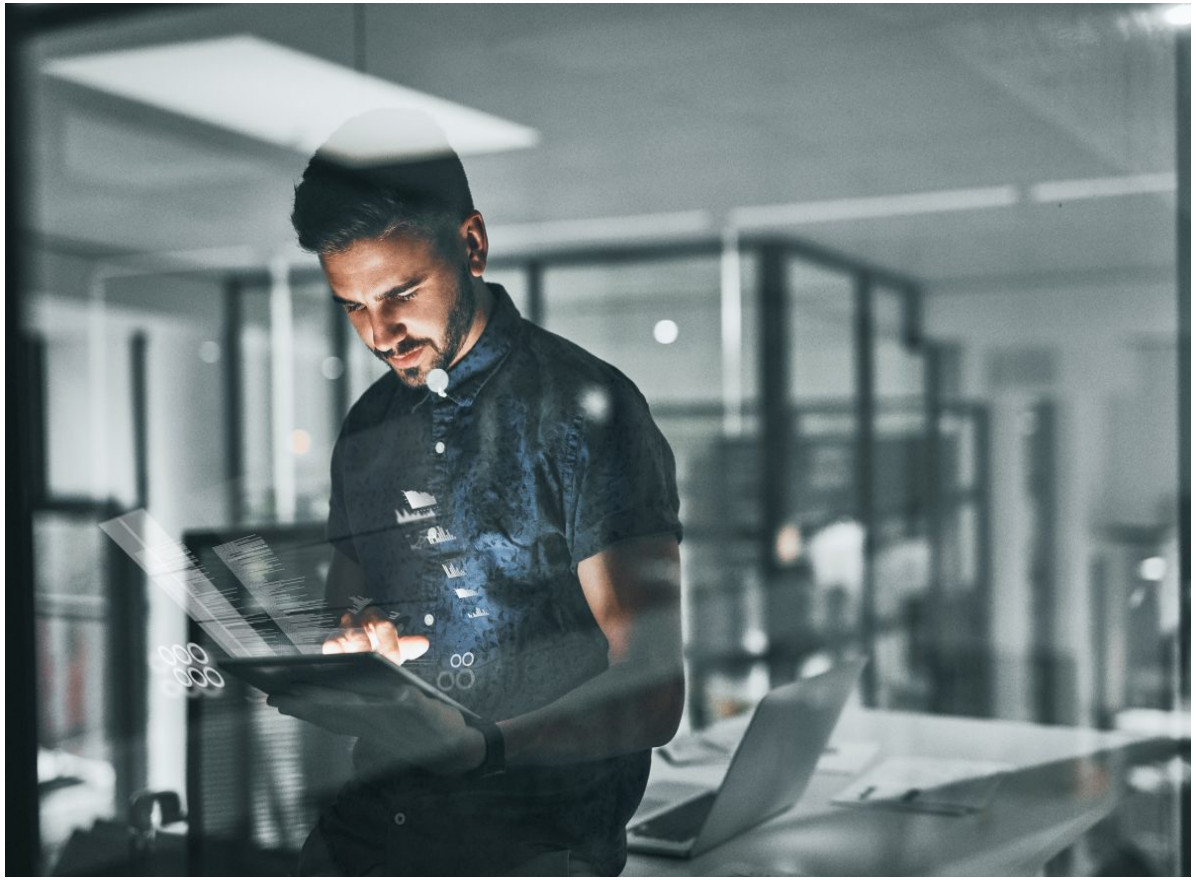
| | |
|---|---|
| **Frequency** | 849 incidents, 571 with confirmed data disclosure |
| **Top patterns** | Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches |
| **Threat actors** | External (61%), Internal (39%) (breaches) |
| **Actor motives** | Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches) |
| **Data compromised** | Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches) |
| **Top IG1 protective controls** | Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6) |
| **What is the same?** | The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point). |

# Safeguard protected health information **PHI**

## Are you compliant / Is your data secure ?

- Healthcare organizations must comply with numerous regulations, including HIPAA (1996)
  - HITECH Act (2009)
  - HIPAA Omnibus Rule (2013)
  - …And a growing number of State regulations
- Breach-related violations are increasingly common across the industry:
  - Phishing attacks, hijacked websites, viruses, ransomware, etc.
  - Breaches can lead to patient safety issues and revenue loss; monitoring for cyber-attacks is a 7 X 24 X 365 job
  - 53% of reported breaches were the result of a malicious attack, with goal to make a profit the aim in most attacks.

- **HIPAA violations can be costly!**
- **Compliance is key for both privacy and security**
- **HIPAA "compliant" is not the same as "data secure"**



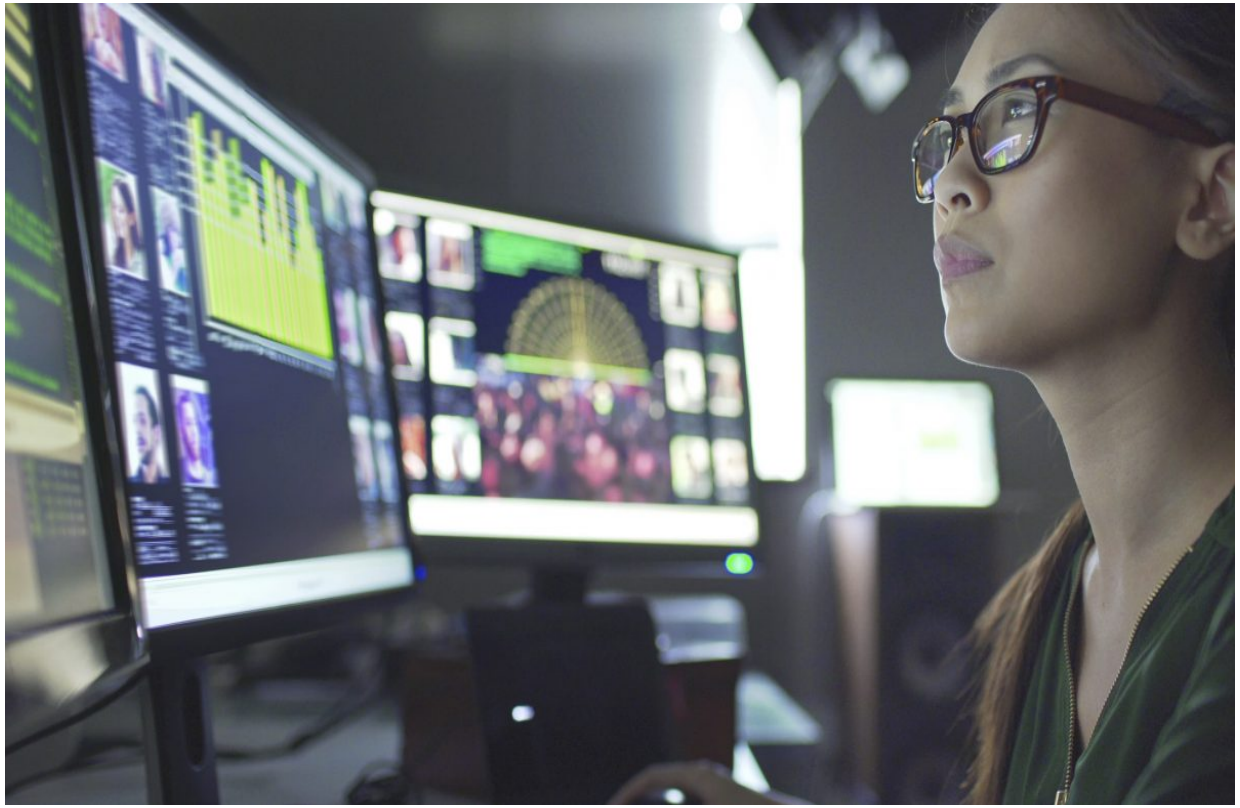
# Safeguard protected health information **PHI**

## Can you trust your vendors to secure PHI?

Because healthcare organizations are also responsible for complying with all Medicare and state public health regulations, providers should require, as part of their compliance program, that their vendors provide assurances that they fully comply with HIPAA regulations and industry best practices for safeguarding of PHI.

But how you do you know for sure?

- 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
- Don’t overlook focus on fourth parties
- Require annual external audits of critical third parties



# Safeguard protected health information **PHI**

## Manage 3rd party risk to ensure privacy & confidentiality

- Healthcare organizations outsource numerous processes and services, but they remain legally accountable for the safeguarding of their patient's data (PHI)
- 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 / non-compliant BAAs

**Common security rule violations**

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

# Safeguard protected health information
# PHI

## Healthcare organizations need a comprehensive information risk management and compliance program

**How can healthcare organizations ensure their data and (by extension) business is appropriately protected?**

- **Regulatory compliance requirements (at a minimum):**
  - HIPAA SR, PR, BN
  - CMS
  - PCI DSS
  - CCPA, GDPR
- **Maturity models (e.g., NIST, HITRUST)**
- **Third party risk management via SOC 2, HITRUST i1**

02

Protecting business

# **Risk assessment**

Option 1

# Stay HIPAA Compliant with a risk assessment

While compliance with privacy regulations is mandatory, it is usually not enough to protect an organization against data breaches. Conducting a risk assessment specifically aimed at HIPAA compliance is an essential step to keep PHI safe while avoiding breaches and penalties for violations.

## Items for consideration

- A risk assessment is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate
- Providers should perform a holistic assessment of the threats facing the organization and the vulnerabilities in its current operating environment.
- Risk assessments can do more than just help organizations stay compliant; they can help providers and others who have access to PHI address possible vulnerabilities outside of the regulations.
- For providers, regular (i.e., at least annual) risk assessments are essential.

## What is a risk assessment?

- A comprehensive look at a healthcare organization's security posture and structure 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 a healthcare organization

# HIPAA risk assessment template

HHS does provide guidelines to ensure that the risk assessment helps organizations understand how their technologies and strategies line up with HIPAA and implement the necessary security measures in their operational environment. HHS lays out the aims of a HIPAA risk assessment for healthcare organizations as follows:

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

# Tools for HIPAA compliance

There are several toolkits available for organizations that want to assess their HIPAA compliance and security practices around PHI.

## Tools for conducting a risk assessment

- The HHS website can be referenced for guidance on HIPAA Risk Analysis, and provides a wealth of information for small organizations on performing a risk assessment on their own
- The NIST HIPAA Security Toolkit Application, which was developed by the National Institute of Standards and Technology (NIST), assists organizations with understanding the requirements of the HIPAA Security Rule and ways to implement the necessary administrative, physical and technical safeguards to meet those requirements.
- Another self-service tool is the HIPAA Security Risk Assessment (SRA) Tool jointly developed by the Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR).

## Third-party risk assessment?

- It can be difficult — especially for small providers with limited resources — to ensure that an in-house security team has conducted a thorough audit.
- By tapping an outside source to conduct the assessment and provide actionable feedback, the provider can ensure that the assessment touches all places PHI could be lurking and can provide help in closing security gaps.

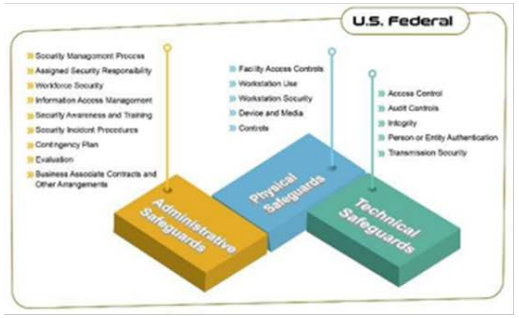
# 03

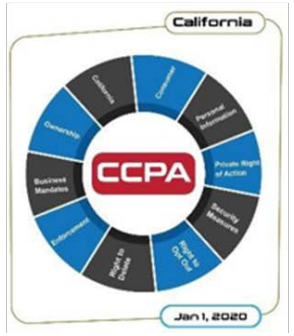
Protecting business

**HITRUST**

# Option 2
# **Becoming HITRUST certified**

- **Reduced Risk** – Ensuring your client has a clear understanding of its data integrity posture so that it can address any weaknesses and reduce its risk now and into the future.
- **Competitive Advantage** – Being able to assure your clients and their customers 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 your client is 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 your client can let its third parties know that it is in compliance and takes data security seriously.



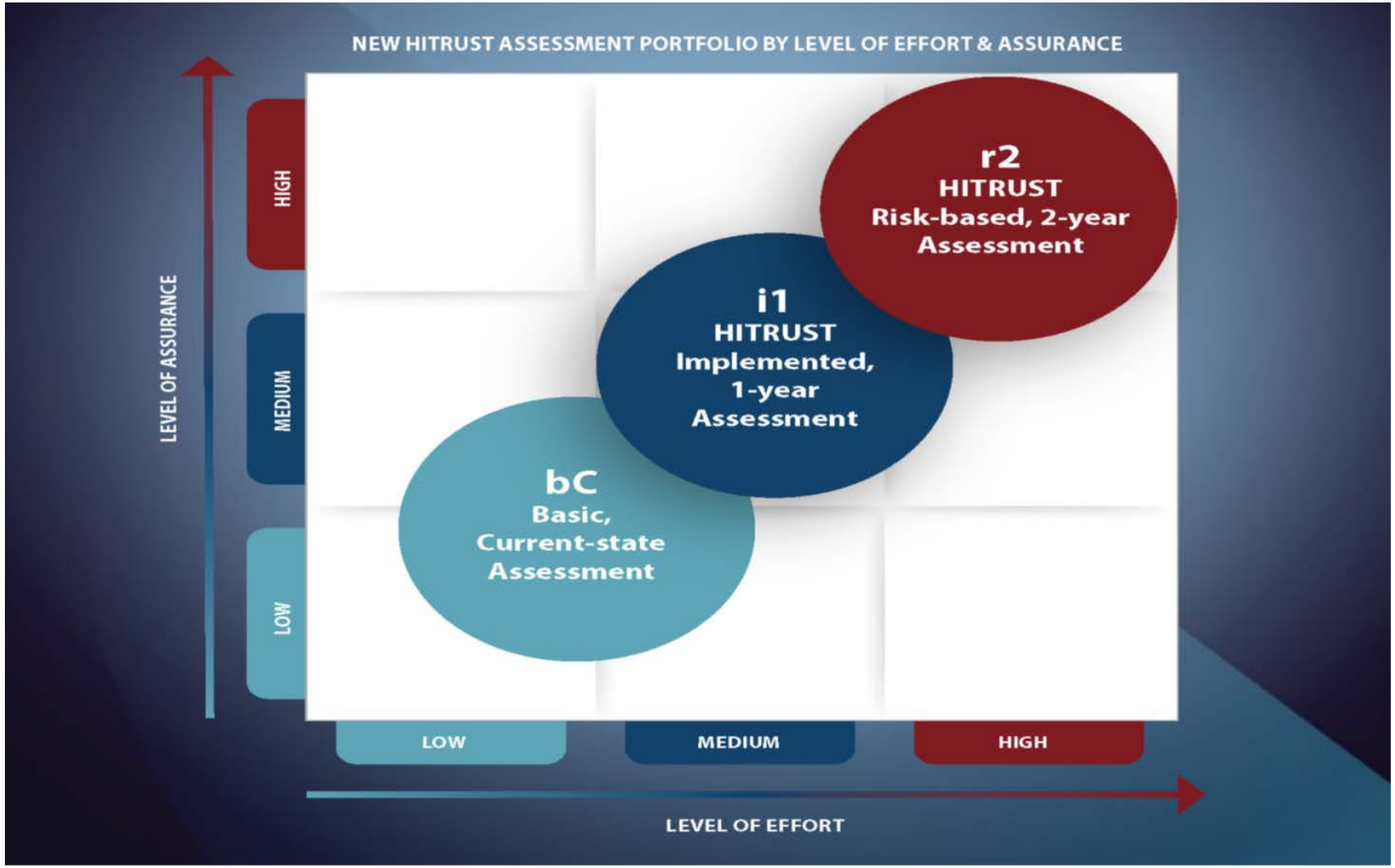

# HITRUST should be the ultimate compliance objective for all healthcare vendors

HITRUST was created by a consortium of 9 healthcare organization to address: (1) concern over data breaches, (2) inconsistent requirements and standards for safeguarding data, (3) compliance issues and (4) the growing risk and liability associated with information security in the healthcare industry.

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


- HITRUST certification is a benchmark for data protection standards in the healthcare field.
- It helps organizations, business associates, and vendors to manage IT risk across all sectors and throughout third-party supply chains.

# HITRUST assessment types




Source: HITRIST

# HITRUST i1 assessment

- Due to the increasing financial and reputational danger for hospitals in the case of a data breach, the Provider Third Party Risk Management Council (PTPRM) now recommends that moderate risk vendors be required to provide information security assurance through the HITRUST i1 certification, rather than through other third-party assurance mechanisms.
- Many hospitals and healthcare organizations are adopting the HITRUST i1 for themselves and their vendors. It is critical to show that your organization is keeping PHI/sensitive data protected and that information security is a top-priority.


- The HITRUST r2 Validated Assessment + Certification is considered the gold standard for information protection assurances because of the comprehensiveness of control requirements, depth of quality review, and consistency of oversight. For organizations sharing sensitive information, handling high volumes of data, or facing challenging regulatory requirements, a properly scoped r2 Assessment ensures that control requirements are effective and compliant. The r2 offers flexible, tailorable, risk-based control selection to meet the most stringent needs.
- The r2 is a tailorable assessment that focuses on comprehensive, prescriptive, risk-based controls specification and selection with a very rigorous approach to evaluation. These factors combine to ensure that the r2 consistently provides the highest level of assurance for organizations with the greatest risk exposure.

# HITRUST r2 assessment

## Considering another framework or standard? It's likely already mapped to the HITRUST CSF.

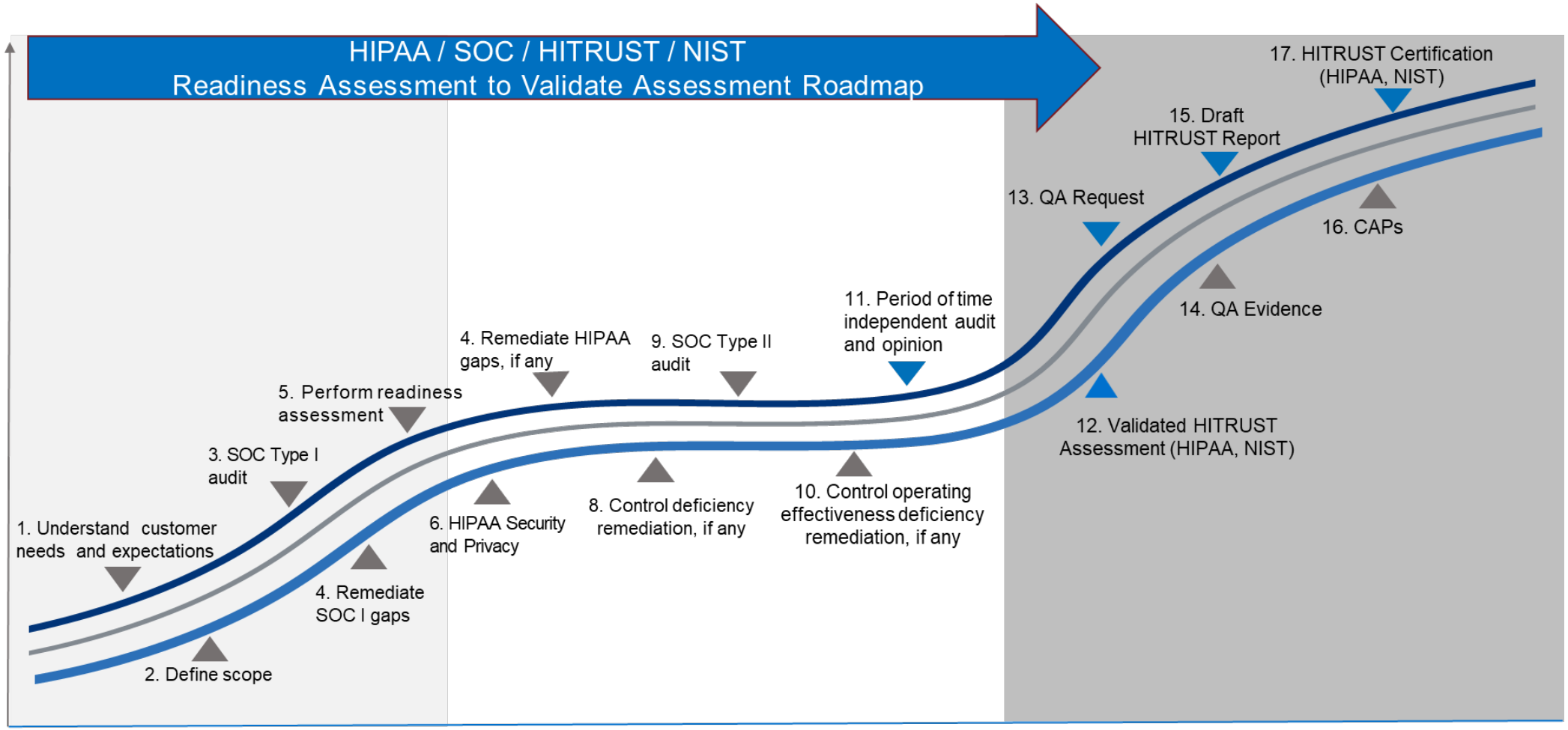
HITRUST has the only solution that integrates 40+ authoritative sources into one certifiable framework, allowing assess once, report many.

| Current Authoritative Sources Included in the HITRUST CSF: | | | |
|---|---|---|---|
| 1 TAC 15 390.2 | CCPA 1798 | HITRUST De-ID Framework v1 | NYS DOH SSP v3.1 |
| 16 CFR 681 | CIS Controls v7.1 | IRS Pub 1075 (2016) | OCR Audit Protocol (2016) |
| 201 CMR 17.00 | CMS ARS v3.1 | ISO 27799:2016 | OCR Guidance for Unsecured PHI |
| 21 CFR 11 | COBIT 5 | ISO/IEC 27001:2013 | OECD Privacy Framework |
| 23 NYCRR 500 | CSA CCM v3.0.1 | ISO/IEC 27002:2013 | PCI DSS v3.2.1 |
| 45 CFR HIPAA.BN | DHS CISA CRR v1.1 | ISO/IEC 29100:2011 | PDPA |
| 45 CFR HIPAA.PR | CMMC v1.0 | ISO/IEC 29151:2017 | PMI DSP Framework |
| 45 CFR HIPAA.SR | EHNAC | MARS-E v2 | SCIDSA 4655 |
| AICPA TSP 100 | EU GDPR NIST | NIST Cybersecurity Framework v1.1 | SP 800-171 r2 |
| APEC | FedRAMP | NIST SP 800-53 r4 | TJC |
| CAQH Core Phase 1 | FFIEC IS | NRS 603A | |
| CAQH Core Phase 2 | | | |

# 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 our clients can focus on the real task at hand: Driving their business.

# HITRUST Roadmap

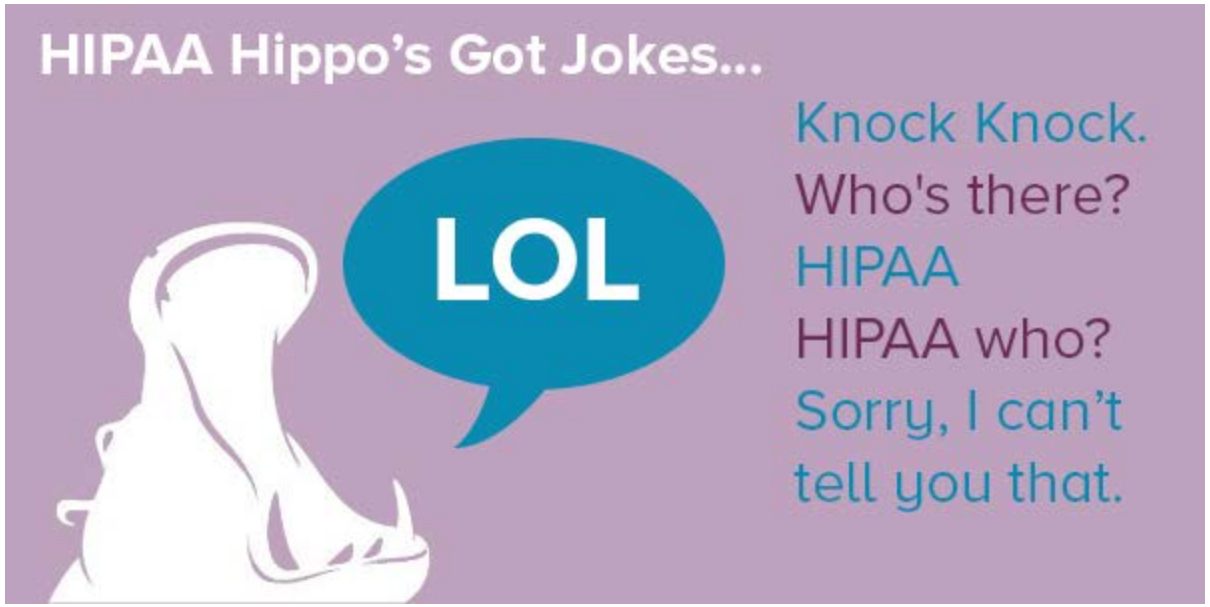


04

# Final thoughts

# Final thoughts

- Many small medical practices have been investigated by OCR and subjected to HIPAA audits.
- In addition, many healthcare organizations – as well as their business associates – overlook the need to conduct a risk assessment from a HIPAA privacy perspective, which is equally as important as conducting a security risk assessment, but typically receives less attention.



# Purpose

The purpose of HIPAA Oversight Service is to establish appropriate administrative, technical, and physical safeguards of Sensitive Protected Health Information including Protected Health Information (“PHI”) and Electronic Protected Health Information (“ePHI”) created, used, or disclosed by our clients.


## Healthcare organizations must find ways to assure that their organization is:

- Maintaining compliance standards
- Educated regarding applicable data integrity requirements
- Have resources to adequately and quickly identify, communicate and correct operational/compliance vulnerabilities
- Meet professional standards applicable to the organization and its core values

# Safeguard protected health information **PHI**

## Five best practices to consider

- Employees are potentially your greatest weakness and greatest asset; single best security investment is security awareness training for your workforce
- Enforce long, complex passwords and use two factor authentication wherever possible; hackers can break passwords 6 characters long in minutes using brute force
- Maintain offline, encrypted backups of your data and ensure you regularly conduct tests of those backups; backups are useless if you can't restore files from them
- Utilize third-party assessments, site visits, and formal certifications to assess your critical suppliers
- Regularly conduct risk assessments – the threat landscape is constantly changing, and yesterday's defenses no longer provide adequate protection

# 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

**Instagram:**
www.instagram.com/mazarsinus

mazars