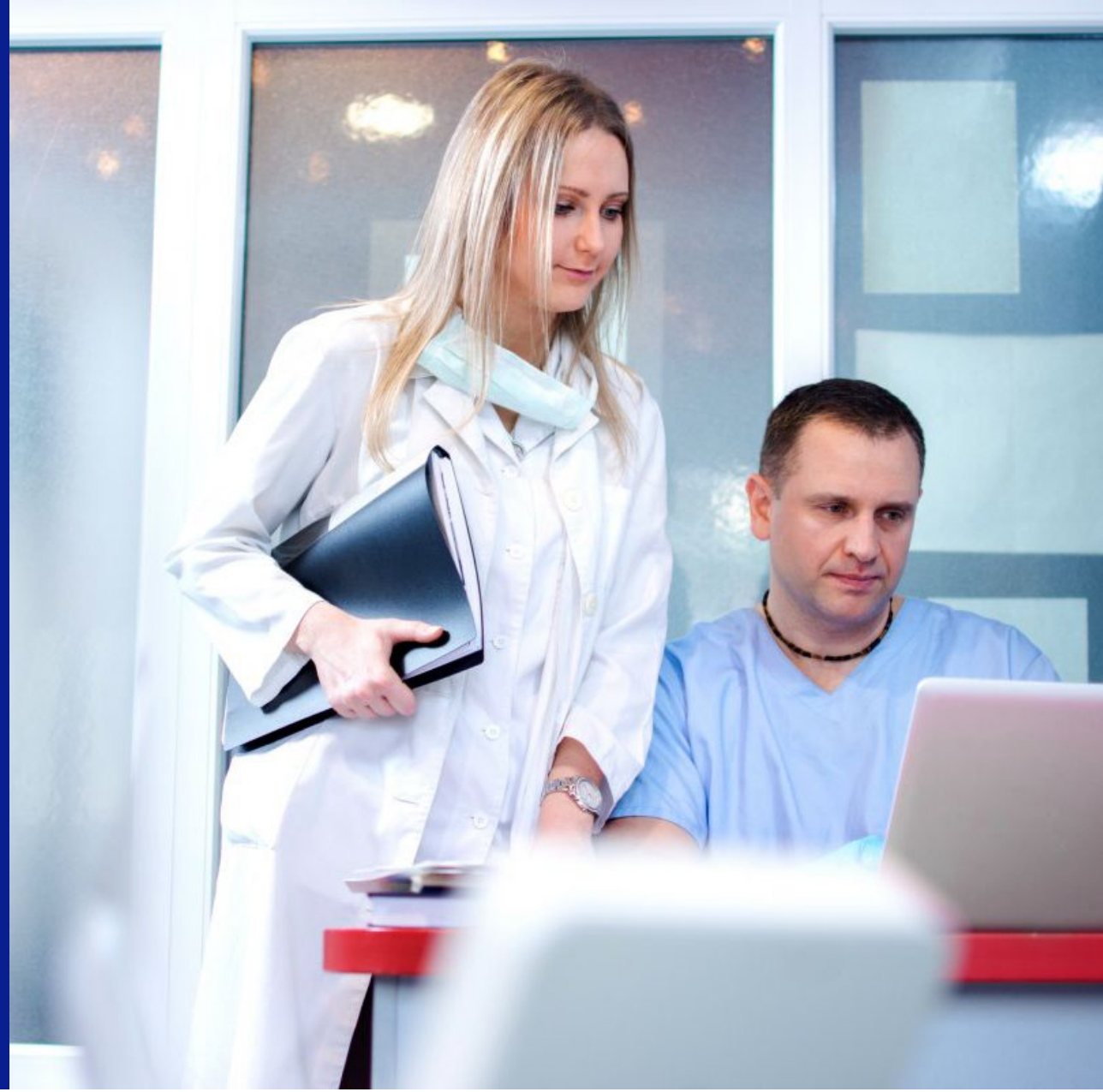
Best Practices for Preventing a Breach

Justin Frazer, Director

October 2022



mazars

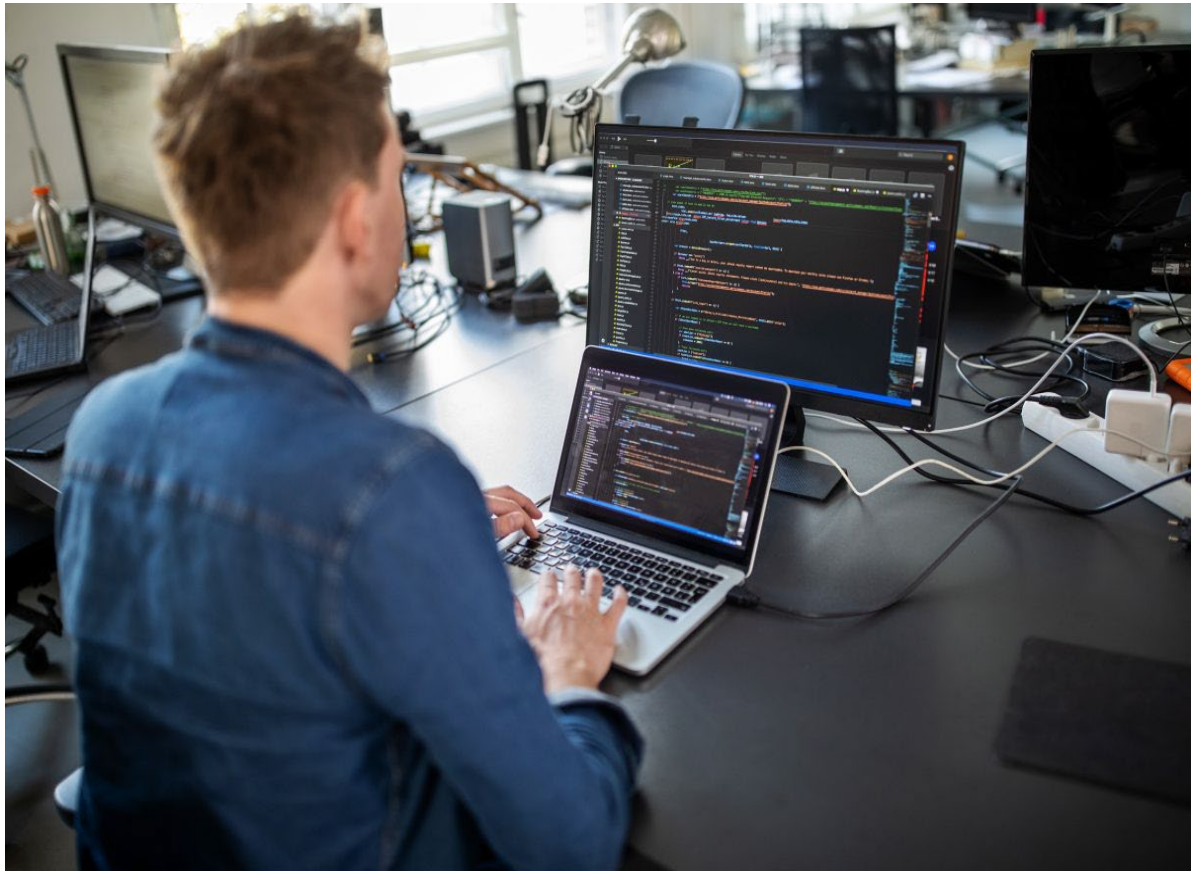
01

A Data Breach Should be Expected

Safeguarding protected health information

Healthcare is an attractive target

- Value of personal health data, ranging from $10 to $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)



Safeguarding protected health information

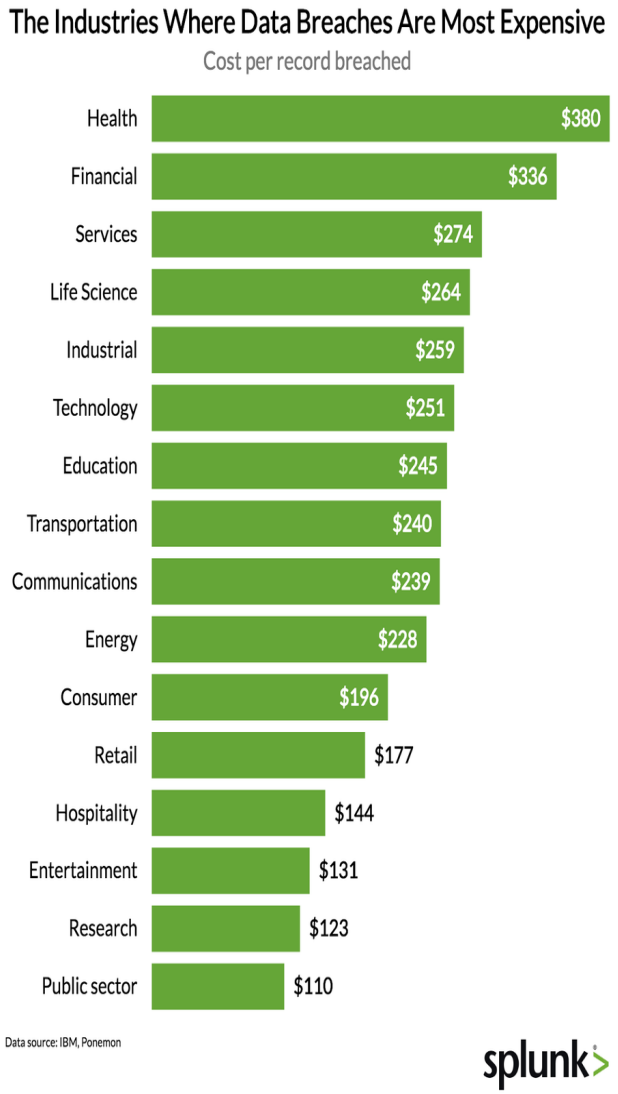
Threat landscape is continuously evolving

- 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 while they remain legally accountable for the safeguarding of their patient's data (PHI)
- A 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 / non-compliant 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?

How can you 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, and timeframes
- Ensure security service level agreements (SLAs) exist in contracts
- Require annual external audits of critical third parties

03

Protecting Your Business with a HITRUST Assessment (for you and/or your vendors)

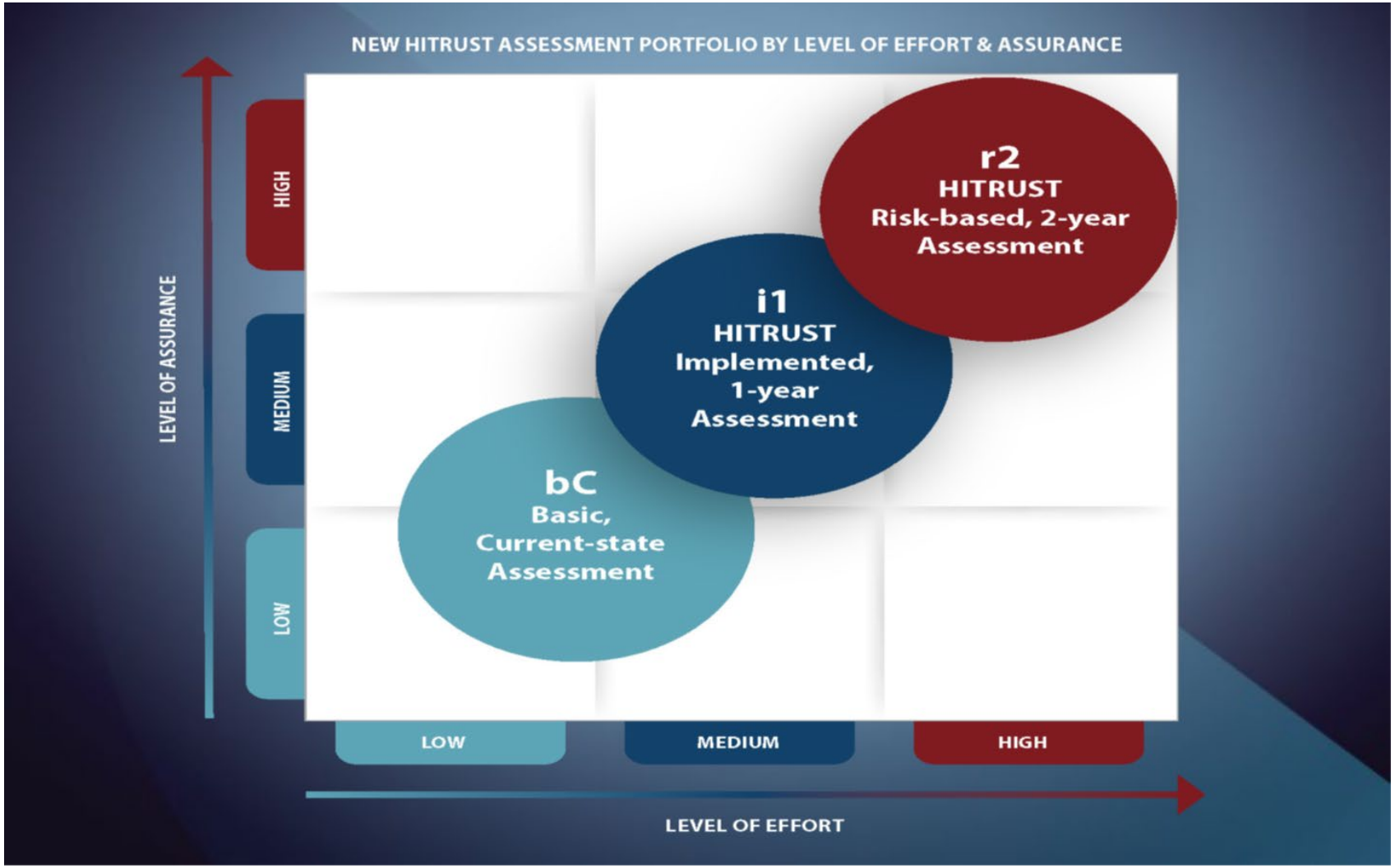
HITRUST should be the ultimate compliance objective for all healthcare organizations

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



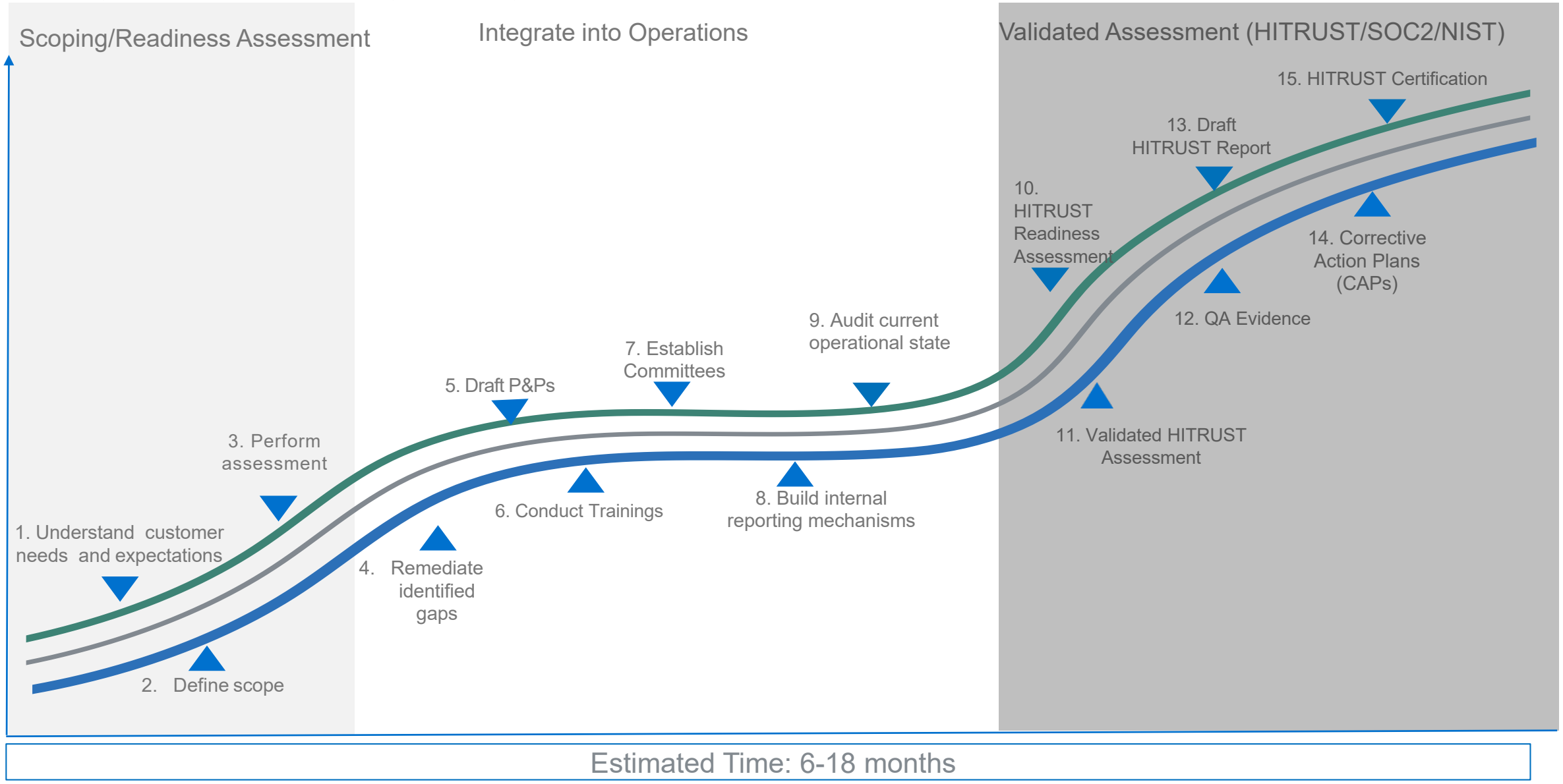
Source: HITRIST

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.

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			

Mapping the HITRUST journey



04

Practices to consider to avoid a breach

Practices to consider to avoid a breach

Annual Security Risk Assessment—HIPAA recommends that providers conduct an annual security risk analysis for vulnerability detection and policy review.

Limit access to health records—Assure that you have effective access permissions depending on user position so that only those healthcare specialists who work with medical records can access them.

Consistent Security Awareness Training—Employees are potentially your greatest weakness and greatest asset; the single best security investment is consistent security awareness training for your workforce.

Document your incident response plan—Creating and implementing a response plan is essential in helping your practice avoid escalations when a breach or incident occurs. This plan will give you clear guidelines for the necessary decisions and follow-up measures.

Create subnetworks—Cyber experts recommend dividing your wireless network into separate subnetworks for different user groups, such as patients, visitors, personnel, and medical devices.

Practices to consider to avoid a breach

Restrict the use of personal devices—The allowance of personal devices used for work has additional risks (esp. in Healthcare). If you allow your employees to bring and use their own phones or other electronic devices for work, create a strict and clear policy that outlines which devices they can use within and outside the network, how to connect them to the network

Update your software regularly—Frequent software updates can correct any of the system's bugs and lower the risk of cyberattacks.

Monitor your vendors—When choosing third-party vendors that will need access to patient data, verify that they comply with HIPAA and other applicable laws. Also have an attorney review your SLAs to ensure that your organization is the sole owner of the data, and you can instantly revoke access when the contract is terminated.

Avoid using outdated IT infrastructure—Older equipment is more likely to be breached. You should consider replacing outdated devices to reduce the risk of data breaches.

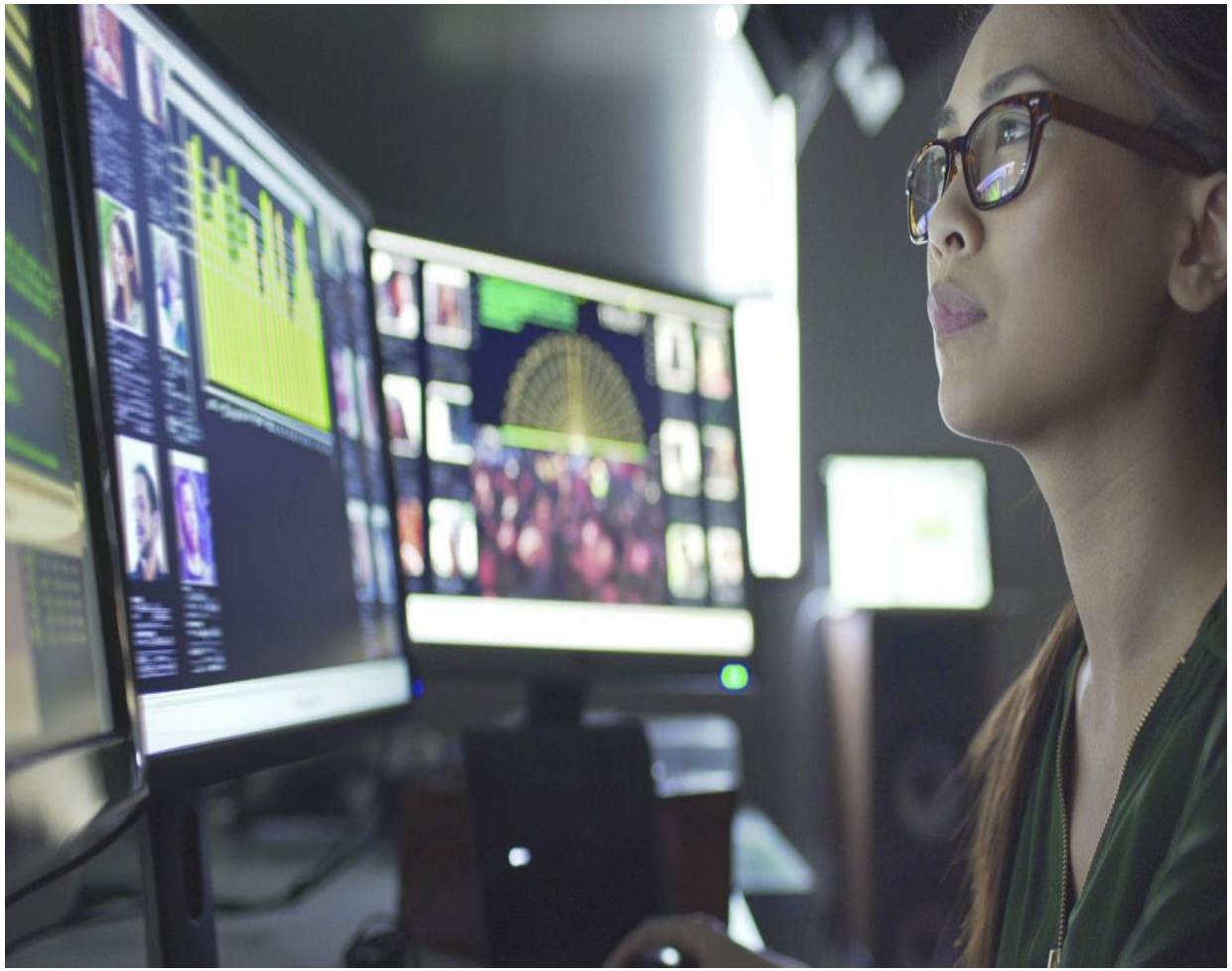
Practices to consider to avoid a breach

Encrypt data—According to HIPAA rules, if encrypted data is compromised, it is not considered a breach. Encryption technologies can significantly help mitigate the consequences of cyberattacks. Encrypting your data now can potentially save your practice from steep government penalties.

Set and enforce retention schedules—A retention schedule is critical to ensure that EHRs containing sensitive stay (or don't stay) in the digital environment longer than required. HIPAA requires six years, but some state laws have a 10-year statue of limitations. Specifically define what to keep, how long and where it is kept.

Destroy sensitive information that does not need to be retained—Some confidential information could be securely destroyed. Consider hiring a reputable document destruction company to assure sensitive information cannot be accessed.

Invest more in your security—The mantra should not be, investing in security "if" we get attacked. Instead, you should invest in security in preparation for "when" you get attacked. It is critical to not only have advanced network security tools, but also strong IT and legal teams.



GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

Something Bad Happened – What do I do?

Stacey L. Gulick, Esq.
Partner
Garfunkel Wild, P.C.

PREPARE

- Before a Security Incident or Breach even occurs, the entity should have a written and detailed incident response plan.
- This is required by the OCR, many health care partners, and cyberliability insurance carriers.
- The Incident response plan can be tested during testing of the entity's disaster recovery plan (such testing is also required by HIPAA)

Remember: the middle of a crisis is not the time to determine who does what.

STOP THE POTENTIAL PROBLEM

1. Whenever possible, as soon as the potential breach is identified, steps should be taken to stop the unauthorized access, use or disclosure (e.g., close a misconfigured port, remove an infected computer from the system, isolate (but don't destroy) an infected server).
2. When taking this step, be careful not to destroy information essential to the investigation of the potential breach (e.g., the identities of the patients affected by the potential breach).

NOTIFY INSURANCE/LEGAL COUNSEL

If at any time during this process, you believe that it is more likely than not that a Breach has occurred:

- Consider notifying legal counsel for assistance
- Identify any potential insurance carrier and put them on alert. In some instances, the insurance company may have specific vendors who can (and must) assist with the process.

IF BUSINESS ASSOCIATE CAUSED BREACH ….

If a Business Associate caused the Breach or security incident, the entity may want to consider whether the next steps should be delegated to the Business Associate.

INVESTIGATE – ESTABLISH RESPONSE TEAM

1. Depending on the nature of the potential breach, the response team may be altered, but in general, the response team should be composed of, at least, the following:
   - Privacy Officer
   - Security Officer
   - IT staff
   - PR staff, if available
   - Operational representative
2. Optimally, the Response Team will already be established in your Incident Response Policy

IDENTIFY A SPOKESPERSON

Identify a spokesperson to handle inquiries from the media, potential hackers, etc. ALL inquiries should go to that person, and only that person.

INVESTIGATE – CONSIDER CONSULTANTS

Consider and engage the consultants that are necessary for the investigation, for example:

- Forensic Consultants
- Legal Counsel
- Breach Coaches

INVESTIGATE – GATHER THE FACTS

1. Take a deep breath!
2. Consider when the potential breach may have occurred and how?
3. Identify which patients may have been affected and what types of information was involved (e.g., clinical vs. financial).
4. Differentiate between whether the information was actually accessed or if it could have been accessed.
5. Try to determine who accessed the information.
6. Determine if the information is still publicly available (if so, you may need to contact third parties to remove).

INVESTIGATE – INVOLVE LAW ENFORCEMENT

If your investigation indicates that there was an intentional intrusion, contacting law enforcement (e.g., State Police, FBI, Homeland Security) may be appropriate.

INCLUDE KEY STAKEHOLDERS

As decisions are made regarding next steps, be sure that key stakeholders (e.g., administrators, medical staff) are aware of what has transpired and what will happen next. In particular, individuals who may receive questions from patients that are notified or the media should know how to respond.

MAKE A DECISION

- Once the facts have been gathered, you will need to be decide whether there has been a breach that is reportable under HIPAA and/or State law.
- Remember, in order not to make notifications pursuant to HIPAA, you must document in a risk assessment that there has been a low probability of compromise.

MAKE NOTIFICATIONS

If you determine a Breach, under HIPAA, has occurred, you must, at a minimum, notify:

- The affected individuals; and
- The OCR (if less than 500 hundred people the OCR must be notified by March 1st, of the year after the Breach occurred)

MAKE NOTIFICATIONS

- Timing is important!!
- Under HIPAA, the notifications to the individuals must be made within 60 days of the date that the incident was discovered or should have been discovered.
- There have been enforcement actions by the OCR for entities that have failed to comply with the 60 days requirement,

MAKE NOTIFICATIONS – MORE THAN 500

- If more than 500 individuals are involved in a HIPAA breach, then you must also notify two media outlets (i.e., two press statements).
- In addition, with that number of individuals, it is likely that more than 10 notifications will be returned so will need to post a statement on your website.
- The OCR will need to be notified as soon as the letters are sent out.

MAKE NOTIFICATIONS – MORE THAN 500

- Consider hiring a vendor to assist with mailing.
- Consider whether credit monitoring should be offered.
- Consider setting up a call center (need to set up a 1-800 number for callers).
- Prepare responses to FAQs.
- Maintain statistics regarding complaints, returned notifications, callers, etc.

MAKE NOTIFICATIONS – STATE REQUIREMENTS

- In many states (e.g., New York), the State law requires that Breaches, as defined by HIPAA, be reported to state agencies as well as the OCR.
- In other states, notification to state agencies is only required if certain information (e.g., social security number) is involved.
- It is usually the residence of the patient that determines which State law is involved.

PREPARE FOR GOVERNMENT INVESTIGATION

If more than 500 individuals are involved, you will be investigated, so you need to ensure that your HIPAA program is compliant:

- Make sure you have an up-to-date risk analysis and risk management plan!!!!!
- Ensure policies are up-to-date and implemented .
- Ensure training has been routinely occurring.
- Ensure staff are prepared to answer questions (e.g., who is the Security Officer? Do you share passwords? Are emails encrypted?)
- Correct any deficiencies you identify.

PREPARE FOR GOVERNMENT INVESTIGATION

You may also be investigated by State Attorney Generals, so be sure to maintain evidence of compliance with all notification obligations.

ANYTHING ELSE?

After the dust settles and all of these regulatory requirements have been met, consider the following:

- Are there any corrective actions to prevent this from happening in the future (e.g., new technical security features, policy changes)?
- Should an updated security risk analysis occur?
- Do any staff need to be re-educated?
- Do any changes need to be made in relationships with vendors?

Note: If the OCR investigates, it will ask for documentation of the foregoing and evidence of these actions can be useful if penalties are proposed.

Questions?