# TAKING A RISK-BASED APPROACH TO HEALTHCARE COMPLIANCE

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY:

## Challenges in Addressing Cyber Risk

Organizations address risk as part of the cost of doing business. However, they often struggle to effectively manage and treat cyber risk across the business. Generally, these struggles range from lacking resources to management's mostly singular focus on prioritizing new business opportunities and initiatives ahead of security. Using this example, management sees the risk of not adapting quickly enough to market trends and potentially missing out on capturing new business or losing market share. In order to keep pace, organizations use automation, distribute workloads, leverage multiple cloud services – often across multiple providers – and contend with an expanding remote workforce. Essentially, while the business is addressing operational risk, cyber risk becomes an afterthought. Further to this point, organizations often view compliance as a business initiative for entering or maintaining market presence and not necessarily tied to managing or maintaining an effective cyber risk posture. This tends to be the case with healthcare organizations and associates.

# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OVERVIEW

The above is especially true in the healthcare industry, where protecting lives, delivering treatments, developing new technologies, conducting clinical trials, and managing this ecosystem is the priority. Nonetheless, the proliferation of patient data coupled with advances in medical device technologies is expanding the scope of cyber risk.

To help with these challenges and encourage organizations to improve their cyber posture, governments worldwide have been developing regulations to set guideposts for managing the data and infrastructure of the healthcare industry and associated entities. In particular, the US government enacted The HIPAA Security Rule, which "establishes national standards to protect individuals' electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity" and requires "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[1] Largely, these safeguards and controls align with Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," from the National Institutes of Science and Technology (NIST).

The HIPAA rule is enforced through the Office of Civil Rights (OCR) within the U.S. Department of Health and Human Services. Generally, a complaint is provided to the OCR, which can choose to investigate. If the OCR determines an entity is not in compliance, it may "decide to impose civil money penalties (CMPs) on the covered entity."[2]

[1] https://www.hhs.gov/hipaa/for-professionals/security/index.html

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html

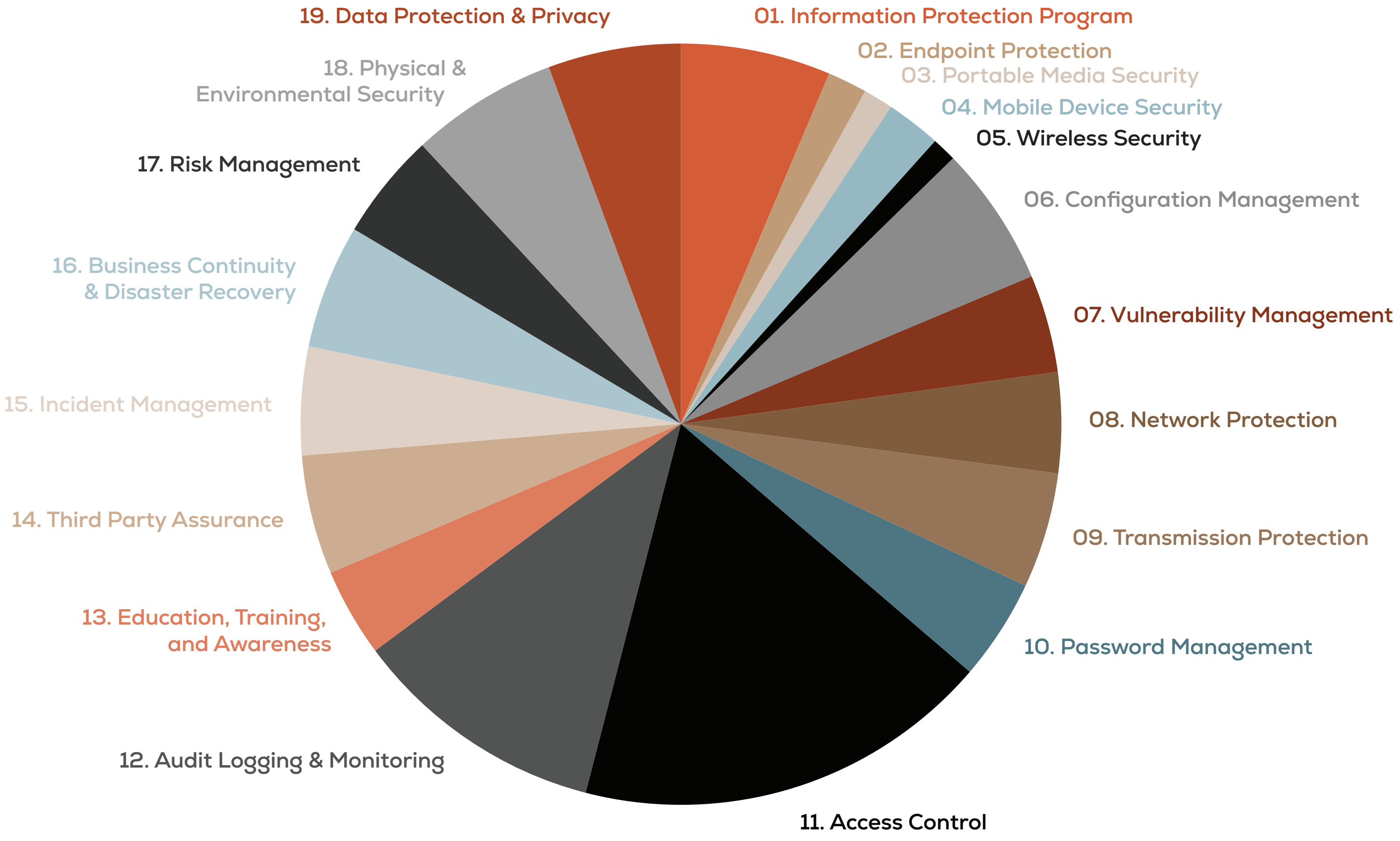
## HITRUST OVERVIEW

Adding another layer of support and guidance, The HITRUST Alliance (https://hitrustalliance.net) has developed a prescriptive set of controls that aid in clarifying the measures an organization must take to align and comply with The HIPAA Security Rule. They take it a step further by offering a certification framework that demonstrates an organization's ability to "achieve, maintain, and provide assurances surrounding the HIPAA Security Rule, HIPAA Privacy Rule, and HIPAA Breach Notification Rule."[3] Becoming HITRUST compliant helps an organization in two key ways:

1. It helps them organize and categorize their HIPAA compliance requirements.
2. In the event of an OCR investigation arising from a complaint or a breach of electronic protected health information (ePHI), proof of HITRUST certification can be used as evidence of in-place controls. The ability to provide this level of control information to the OCR helps speed up the investigation and aids in reducing potential fines and penalties.

Regarding helping organize and categorize compliance requirements, HITRUST categorizes controls using 19 control domains in which specific control requirements are organized. Using this model, organizations can map controls requirements and their associated effectiveness.

### HITRUST Controls Chart



[3] https://hitrustalliance.net/hitrust-for-hipaa/

# MAPPING CONTROL REQUIREMENTS

One of the first things an organization should understand is their regulatory and/or compliance obligations. Once these are defined, the organization needs to identify the regulatory/compliance requirements and scope of the regulated environment. Identifying scope centers on understanding what regulated data is being collected along with where and how it's stored. Once the in-scope environment is confirmed, the organization can then align and assess the required controls. Typically, compliance control requirements map to regulatory requirements. This is the case with HITRUST and The HIPAA Security Rule as outlined below.

| Factor | ISO/IEC 27001 | NIST SP 800-53 | HITRUST CSF |
|---|---|---|---|
| ISO 2700-Based | ✓ | ✗ | ✓ |
| Integrated Compliance Framework | ✗ | ✗ | ✓ |
| Prescriptive | ✗ | ✓ | ✓ |
| Controlled Scaling | ✗ | ✗ | ✓ |
| Controlled Tailoring | ✗ | ✓ | ✓ |
| Controlled Compliance-Based | ✗ | ✓ | ✓ |
| Organizational Certification | ✗ | ✓ | ✓ |
| Supports Third-Party Assurance | ✓ | ✗ | ✓ |
| Assessment Guidance | ✗ | ✓ | ✓ |
| Tool Support | ✗ | ✓ | ✓ |

## Key Takeaway

Of particular note when reviewing control requirements is a common thread – cyber risk. It is called out specifically by name in HITRUST Domain 17 "Risk Management" and is relevant when addressing many of the other domains. Whether addressing network controls (HITRUST Domain 8 – Network Protection), developing incident response capabilities (HITRUST Domain 15 – Incident Management), or defining data protection strategies (HITRUST Domain 19 – Data Protection and Privacy), reducing the risk to unauthorized or accidental disclosure or loss of sensitive data (i.e. ePHI) is paramount.

This is where taking a risk-based approach can make an organization's compliance obligations easier to manage. For example, knowing what sensitive data exists and where helps an organization understand their potential exposure to fines and penalties. This then empowers the organization to deploy protective measures to reduce the likelihood of an adverse event where there's a loss or disclosure of ePHI, and thus reducing organizational risk. Further, when deploying these risk mitigating measures, the organization is now better positioned for earning and maintaining compliance.

The opposite approach of addressing compliance control requirements often leads to a whack-a-mole scenario where the organization is managing their security controls through the lens of compliance obligations. This creates challenges, as the organization will then chase specific compliance control gap items, potentially taking attention away from other items that expose the organization to more risk. As an example, HITRUST Certification requires a heavy amount of documentation. However, if an organization is focused on developing or enhancing their documentation, they may not be tightly focused on practicing good network security measures, which could lead to a breach or loss of ePHI. This is where taking a risk-based approach is particularly helpful:

1. Knowing that protecting the network decreases risk to a higher degree than ensuring that all the documentation is up to snuff.
2. Prioritizing risk reduction actions and treatments more holistically and efficiently.

## KEEP IT SIMPLE – FOCUS ON THREE

NIST SP800-53 and the NIST Cybersecurity Framework (NIST CSF) both focus on three key areas: Protection, Identification, and Response. In fact, the NIST CSF domains specifically call out these three as part of the five domains (Identify, Protect, Detect, Respond, Recover). Further, the majority of the control and safeguard requirements included in NIST SP800-53 are designed to enforce these tenets, whether it is implemented technologies or the processes and procedures. Keep in mind that both HIPAA and HITRUST base their compliance requirements on this framework.

### Protect

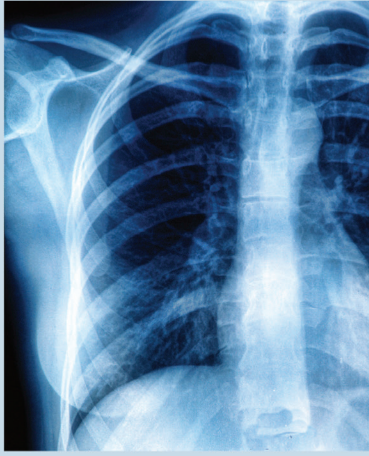
Of the over 1,000 controls included within NIST SP800-53, roughly forty percent use language discussing and requiring the protection of systems and data. Although many of these control requirements center on policy or procedure, the fact remains that protection is core to not just safeguarding systems and data, but also to gaining and maintaining compliance.

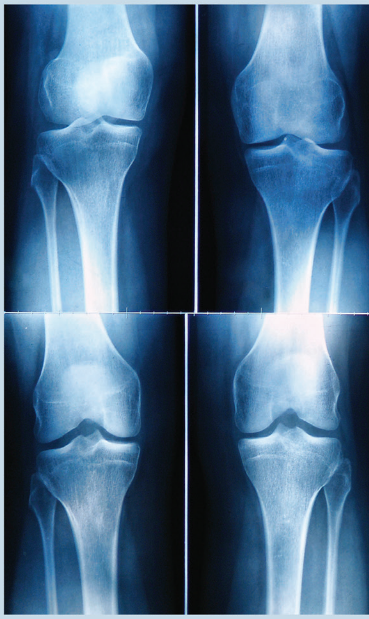
### Identify

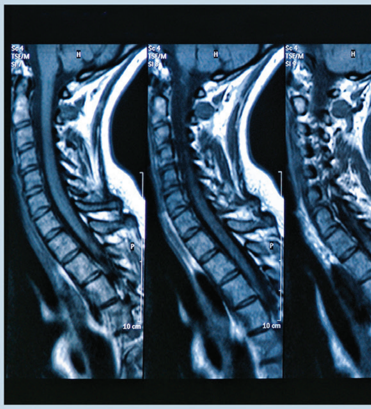
There are 115 separate controls within NIST SP800-53 that focus on identification of authorized and unauthorized systems and users. These controls can be separated into two groups: (i) identification of processes or procedures that support the authentication and (ii) authorization to systems and data and identification of unauthorized systems or user access. Mainly, the ability to identify unauthorized or suspicious activities supporting the organization's technical ecosystem is the principal focus of this area.

### Respond

Although containing the smallest number of SP800-53 controls at 42, it's arguable these may be the most critical. When an organization is dealing with a cyber incident or event, its ability to respond and correct the matter efficiently and effectively is paramount to limiting damage. Additionally, these controls are more procedural based, focusing on the organization's response plans and capabilities. It should be noted that these are based on support from notifications arising from protective and identification measures the organization has in place.







# HYAS SOLUTIONS – ENABLING COMPLIANCE AND REDUCING RISK

The HYAS solutions, HYAS Insight and HYAS Protect, when used together can greatly aid healthcare organizations and associates in gaining compliance and reducing risk to potential cyber incidents. The abilities these services offer – identifying and protecting the organization from unauthorized and unwanted traffic – also reduce risk to ransomware attacks, supply-chain attacks, and data breaches.

## HYAS Protect

HYAS Protect helps organizations block attacks before they happen. This is accomplished through HYAS' proprietary attacker infrastructure data aggregation platform. When implemented as part of an organization's defense and compliance strategy, attacks are preempted by the blocking of the communication infrastructure (often referred to as command-and-control or C2) used by malicious actors to launch their attacks. The ability to block attacks preemptively reduces the likelihood of a breach, thus reducing the organization's cyber risk.

HIPAA and HITRUST compliance requirements include numerous controls on securing DNS and blocking unauthorized communications between systems or users that are mandated. Virtually all the control requirements within the System and Communications Protection (SC Controls identifier) can be satisfied with the HYAS Protect solution. More specifically:

**SC-7:** Boundary Protection
**SC-20:** Secure Name/Address Resolution Service (Authoritative Source)
**SC-21:** Secure Name/Address Resolution Service (Recursive or Caching Resolver)
**SC-22:** Architecture and Provisioning for Name/Address Resolution Service

## HYAS Insight

HYAS Insight assists organizations in identifying attacker infrastructure and attack attributes, enabling organizations to improve their threat intelligence and enhance their abilities to rapidly respond and investigate potential cyber incidents and events. Leveraging this information, organizations are able to identify indicators of compromise (IOCs), limiting exposure to breach or ransomware and reducing their overall cyber risk.

When taken in the context of compliance, there are 121 controls that specifically call out “threat.” Although many of these address procedural items like training and awareness, the majority cover specifically being able to identify and block threats from negatively impacting the organization. A few examples include:

**AC-13(3):** Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

**IR-4(4):** Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

**RA-10:**
**A.** Establish and maintain a cyber threat hunting capability to:

**1.** Search for indicators of compromise in organizational systems; and

**2.** Detect, track, and disrupt threats that evade existing controls; and

**3.** Employ the threat hunting capability [Assignment: organization-defined frequency].

**SI-3(10):**
**A.** Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and

**B.** Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

## CONCLUSION

Approaching compliance implementation and the management of cyber risk as separate initiatives actually makes the overall process and implementation more complex and challenging. This is especially the case in the healthcare industry where HIPAA controls and HITRUST compliance are not just barriers to market entry but are requirements to handling patient data. Further, taking a linear approach to meeting each control is time consuming and expensive. However, taking a risk-based approach to enterprise cybersecurity enables an organization to:

1. Properly scope their controlled environment
2. Reduce complexity in managing and maintaining compliance requirements
3. Address and treat cyber risk based on potential liability or cost
4. Be more flexible with changing compliance requirements
5. Reduce cost when managing organizational cyber security

HYAS

## ABOUT HYAS

HYAS is a valued partner and world-leading authority on cyber adversary infrastructure and communication to that infrastructure. We help businesses see more, do more, and understand more about the nature of the threats they face, or don't even realize they are facing, on a daily basis. Our vision is to be the leading provider of confidence and cybersecurity that today's businesses need to move forward in an ever-changing data environment.

## FOR MORE:

✉ **info@hyas.com**

🖥 **hyas.com**