



Health Sector Coordinating Council  
Cybersecurity Working Group

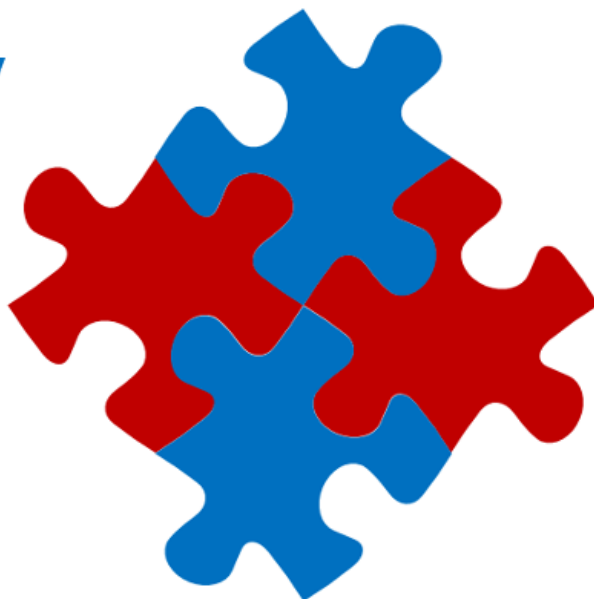


Manage  
Risks

Health Industry Cybersecurity -

# Coordinated Privacy and Security Partnerships (CPSP)

Privacy



Security

FEBRUARY 2024

---

## Table of Contents

Executive Summary	4
Introduction	5
Purpose and Intended Use of Publication	6
About the Health Sector Coordinating Council Cybersecurity Working Group	6
Acknowledgements	6
Importance	7
Definitions	8
Organizational Reporting Structures	8
Survey Summary	9
Board Oversight of Privacy and Security Risk	10
Common Reporting Structures	11
Challenges between Privacy and Security and Organizational Risk	13
Best Practice Strategies for Privacy and Security Interconnection	16
Use of Responsibility Assignment (RACI) Matrix	19
RACI Template	20
Organizational Structure Considerations for Privacy and Security	28
Organizational Reporting Relationship Pros and Cons Table	29

---

Privacy Intersection with Security Practices	32
HICP	33
Privacy Engagement with Health Industry Cybersecurity Practices (HICP)	34
Crosswalks of NIST Frameworks	38

---

---

## Executive Summary

Healthcare, as a recognized critical infrastructure, is comprised of various entity functions:

- Delivery of direct patient clinical services by providers, medical systems, laboratories;
- Health plans and payers;
- Pharmaceuticals, medical materials, and health information technologies;
- Public health entities; and
- Federal partners, coordinated response providers, and emergency services.

Whether an enterprise is small or large, the care and safety of patients and healthcare consumers are at the center.

Patients and healthcare consumers trust and expect that:

- Their confidential and sensitive data is being acquired, used, disclosed, and protected in accordance with applicable laws, regulations, and best practice standards;
- They can exercise certain transparent rights and control over the availability, accessibility, and interoperability of their data;
- The data kept about them is accurate such that health entities can make fully informed decisions; and
- Their clinical health outcomes, safety, quality of care, and privacy are not impacted by a cybersecurity event.

The board of directors and senior executives trust and expect that:

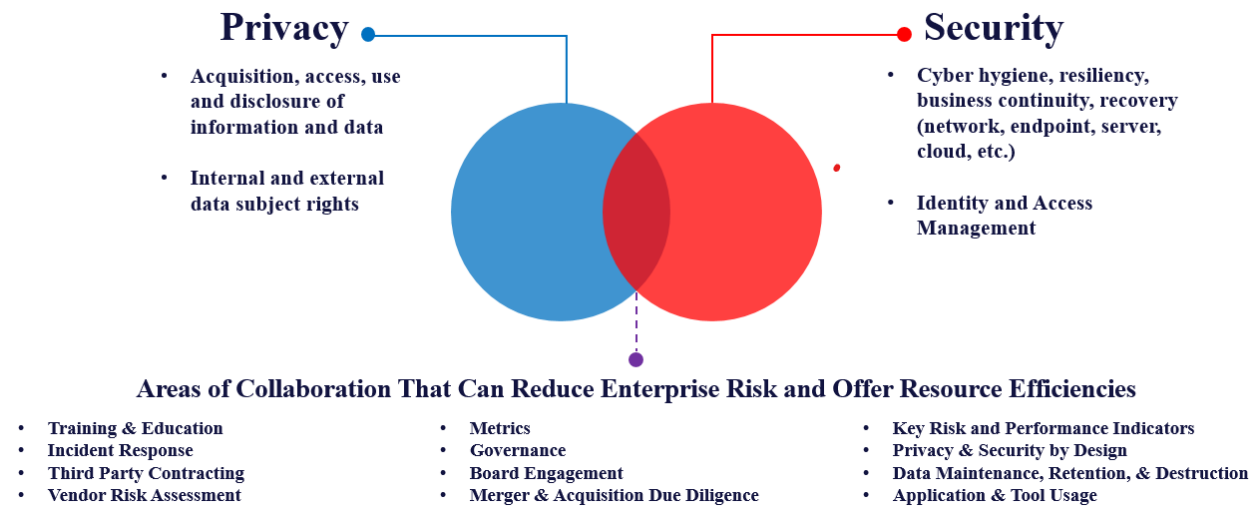
- Patients and consumers remain safe;
- Applicable laws and regulations are understood and followed by the business;
- The business mission, vision, and strategic priorities are being supported and carried forward through corresponding departmental strategies, governance, and feedback metrics;
- Known risks and vulnerabilities are identified and mitigated to offer protections; and
- Human, financial, and other resources are being effectively and efficiently used.

Through the interpretation of complex and ever evolving laws and regulatory landscapes, Privacy and Security are the areas tasked with implementing policies and controls that govern data protection. They execute interdependent and cross-functional principles, frameworks, and strategies in an attempt to protect data, keep patients safe, and the business operational from threats.

This resource provides information about challenges contributing to increased entity risk, that can occur between Privacy and Security, despite having the same protection goals when:

- The language or frameworks used are misunderstood operationally by each resulting in team dynamic difficulties, redundancy of efforts, or poor execution of incident response measures when time is of the essence;
- Company tone, culture, or board oversight is inadequate leading to misaligned reporting structures, lack of adherence to strategic goals, inconsistent policies and procedures; or
- Regulations are misinterpreted which can inadvertently set the entity up for non-compliance and implicate audits, fines, or other corrective actions.

More importantly though, this document highlights the ways that Privacy and Security can proactively and cohesively work together. It provides practical suggestions of collaborative practices seeking to accomplish this in the interests of the patient and the enterprise alike through the use of shared executive sponsorship, combined governance, and tabletop exercises, as a few examples. The infographic provides an overview of basic areas of coverage for Privacy and Security with twelve (12) areas for partnership providing ways to influence efficiency and potentially reduce enterprise risk.




---

## Introduction

It is often misunderstood that Privacy and Security function within separate and distinct silos within the healthcare and public health sectors. In actuality, Privacy and Security have much in common. A sound Privacy program necessarily includes requirements for appropriate cybersecurity practices to protect sensitive data. Security teams must consider Privacy principles to establish appropriate standards for Security measures. However, there remains a lack of shared understanding of operational definitions, clear roles and responsibilities, reporting relationships, a coherent enterprise framework and regulatory interpretations. This disconnect can lead to inefficiencies, compliance gaps, and increased organizational risk. This amplified risk can have significant consequences for patients, consumers, the public, and the organization itself.

For Example:

- A Security team focused only on risk to an organization’s systems may overlook assessing whether the data elements shared with a third-party vendor are more than the minimum necessary or they may not recognize some of the elements as protected health information (PHI). This could lead to more data being provided to the vendor than is necessary for the given purpose and therefore, under applicable laws and regulations, potentially leading to a more impactful incident with increased consequences.
- A Privacy review of contractual documents may allow for edits while contracting with a third-party that, while minimal from a Privacy perspective, introduce unwanted and unnecessary Security risks into the organization’s network or allow uses and disclosures of data by the vendor that were not anticipated.

---

## Purpose and Intended Use of Publication

The Health Sector Coordinating Council Cybersecurity Working Group (HSCC-CWG) developed this resource on the proposition that enterprise Privacy and Security compliance functions are inherently interdependent and reinforcing, yet organizationally less coordinated than efficiency and risk reduction would optimally require. As cyberattacks and data breaches of private information continue to increase in both frequency and severity, there is significant evidence that neither regulations nor enterprise compliance and risk management programs approach these interdependent responsibilities with coherent and coordinated policy and practice. The intended audience for this document includes healthcare Privacy, Security, and Compliance leaders, their accompanying teams, and others looking to develop best practices for Privacy and Security programs and policies.

This publication seeks to do the following:

- Identify intersections, interdependencies, and regulatory and operational distinctions between enterprise Privacy and Security disciplines;
- Enumerate potential challenges and corresponding risks arising from gaps and/or misalignments between Privacy and Security functions and priorities;
- Describe differing structural advantages and disadvantages for coordinating or integrating functions; and
- Recommend options for frameworks, practices, and measures that can assist with informing, coordinating, and integrating Privacy and Security compliance and operations efforts.

---

## About the Health Sector Coordinating Council Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with multiple federal, state, international, and local government agencies to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

---

## Acknowledgements

The Health Sector Coordinating Council expresses its gratitude to the many member representatives who worked as part of the Privacy and Security Task Group and contributed significant hours and discussion to the development of this resource. The Privacy and Security Task Group met weekly in various subgroup and larger group formats over the course of eight months to develop, solicit and adjudicate feedback, write, and complete this publication.

In particular, we wish to thank the following individuals who volunteered as a “Strike Force” to provide direct thought leadership and draft the content in this document.

**Mike DeGraff (co-lead)**

The Joint Commission

**Troy Adams**

U.S. Dept. of Health and  
Human Services, HC3

**Chris Logan**

Censinet

**Nick Heesters (co-lead)**

U.S. Dept. of Health and  
Human Services, Office for Civil  
Rights

**Michael Alicia**

Business Intelligence Group

**Andrea McColl**

University of California Los  
Angeles Medical Center

**Karen Habercoss (co-lead)**

The University of Chicago  
Medicine & Biological Sciences

**Preethi Amurthur**

Philips

**Diah Ramesh**

Abbott

**Jessica Kosteva (co-lead)**

The Johns Hopkins Health  
System

**Chris Brandt**

Premera Blue Cross

**Erica Riethmiller**

University of Colorado Health

**Haris Domazet**

Epic System Corporation

**Frank Ruelas**

CommonSpirit Health

**Ed Gaudet**

Censinet

**Christine Sublett**

Sublett Consulting

---

## Importance

Privacy and Security functions are each driven by public expectations, business objectives, laws and regulatory requirements to, among other goals, ensure individual rights and the confidentiality, integrity and availability of data. The need for coordination between Privacy and Security is an important factor not just for compliance, but also for patient safety and an organization’s reputational value and trust. It is also crucial to safeguarding patient information and mitigating the risk of harm, as well as actual harm, caused by cyber threats. Patient health information is uniquely sensitive because unlike a credit card number it cannot be easily replaced, and if compromised it can be leveraged for medical identify theft or other nefarious purposes.

However, the national imperatives of data interoperability and patients’ rights to their electronic health information for more efficient and patient-centric healthcare can introduce real or perceived tensions between Privacy and Security. These tensions can engender lack of trust, poor communication, misunderstood goals and objectives, unclear scopes of or gaps in responsibility, conflicting priorities, unequal or insufficient resource allocation, misalignment of risk mitigations and differentiated tolerance for risk acceptance. Finding and developing the optimal and relevant areas where Privacy and Security should collaborate is a key to addressing these tensions.

The march of innovation further requires strategic forethought into deployment, architecture and use policies for emerging technologies. Consider, for example, how new technologies such as artificial intelligence, blockchain, and quantum computing all show demonstrable threats to and benefits for both Privacy and Security goals. Starting the conversation with awareness of the shared priorities of protecting patient data while ensuring secure operations allows each to appreciate the necessity for early and frequent engagement.

---

## Definitions

The balance of Privacy and Security roles in healthcare requires the negotiation of many factors. Due to the complexity of scope, scale, and defining the relationship between responsibilities of both disciplines is a difficult task. Such definitions must allow for broad application across the healthcare space and among various regulatory frameworks and roles. In practice, Privacy and Security must work in tandem to assure the understanding of the various rules and regulations facing the organization, and how they apply to the organization's environment. This is necessary to develop effective and comprehensive compliance plans and program strategies.

Privacy roles support compliance with existing laws, regulations, standards, and practices, and mandate and monitor existing internally developed Privacy policies and procedures. This may be accomplished through education and training, discovering gaps, and establishing new Privacy policies governing the protection, collection, management, and handling of electronic and physical personal and medical information. The Privacy role works from both technical and non-technical stances to ensure that Privacy risks are minimized, the organizational risk posture is known, and the overall organization is resilient.

Security roles support the implementation of information safeguards and Security policies by implementing technical, physical, and administrative controls and responding to threats which may compromise the confidentiality, integrity and availability of data assets. The Security role works from both technical and non-technical stances to ensure that Security risks are minimized, the organizational risk posture is known, and the overall organization is resilient. Security supports compliance with existing laws, regulations, standards and practices for information Security. The Security role works with the Privacy role to achieve compliance with Privacy laws and regulations.

---

## Organizational Reporting Structures

The reporting structure for the Privacy and IT Security teams within a healthcare organization can vary depending on the organization's size, culture, healthcare vertical, and other needs of the organization. There is also reliance on other teams, Health Information Management, Clinical Informatics, Compliance, and Legal as examples, to help administer the privacy and security rules. Regardless of structure, many regulatory and practical needs bring Privacy and Security functions together. Organizational structure is certainly not the only driving factor behind a successful working relationship between Privacy and Security, but it can definitely facilitate or hinder the effectiveness of both programs.

For example, some organizations have Privacy reporting to the Legal or Compliance departments and Security reporting to the Information Technology or Risk departments. In some ways this works well: Privacy functions tend



to be more regulatory-oriented, and Security certainly has significant technical or risk components, but it can also lead to both teams taking a silo approach without a common basis for communication or awareness of shared issues. In small entities, when there is a single person handling both Privacy and Security functions, the individual may have strength in only one area or may even have additional work responsibilities related to the overall business operations of the entity such as human resources or revenue cycle. Understanding the risks inherent to any particular structure allows an organization to implement mitigations, such as a recurring meeting cadence or cross-training.

Taking a closer look at an enterprise's structure, particularly in the context of alternatives, can also shed light on possible blind spots, biases, and gaps, and may provide insight into some of the root causes of existing issues. A 2023 Health Sector Coordinating Council Privacy and Security Task Group survey of its members about Privacy and Security structures and reporting relationships identified the more common ways in which current relationships between Privacy and Security are structured across different types of entities throughout the healthcare sector.

---

## Survey Summary

A recurrent theme from survey respondents is when Privacy and Security individuals are willing to put forth effort to work together, any organizational structure can have the potential to be successful. The most successful informal relationship still has risks which can be mitigated by having a formal structure underneath that makes sense for the particular enterprise size, culture, and staff. Changes in leadership or staffing, competing priorities, technical and regulatory knowledge, and budgets among other things can all interfere with a self-directed successful working relationship. For example, while it would make sense for Privacy to be involved in hiring decisions for Security leadership and vice versa, without a clear formal relationship it might not occur to those establishing hiring committees or interview panels to include the other team.

Awareness, understanding, and coordination is not limited just to leadership. In organizations where there are Privacy and/or Security teams, it is critical that the relationships be built at all levels for shared goals to be properly operationalized. While this can be done in any operational structure, it is best facilitated by having both Privacy and Security in a symbiotic configuration, particularly if there can be deliberate processes, such as all-hands meetings where teams discuss issues confronting them, to promote interdisciplinary understanding.

Much of the discussion about organizational structures in this section has focused on structures where Privacy and Security are each considered one entity having a single place within a vertical. However, another approach that some organizations have taken is to break apart the Security responsibility into teams within different verticals. Some organizations have distinctly separate Security teams. One focused on security operations and identity and access management functions housed in IT, and the other on the regulatory and compliance aspects of information security, housed in the same vertical as Privacy (typically Compliance). This Security "Compliance" team is more immersed in matters of Privacy, and in some cases both teams function under a Chief Privacy and Data Security Officer providing guidance to and oversight of the operational teams. Additionally, in global enterprises there may be multiple Privacy

*"When I started as a junior Security team member, our team leader had an effective relationship with Privacy, so I gained a significant amount of functional Privacy knowledge which helped my organization overall. But then Privacy leadership changed, the two teams stopped having joint meetings (except at the top), and the team members we've hired since then became less familiar and with Privacy issues."*

and/or Security teams functioning in different countries or business units that may or may not report to a single and/or separate executive leaders. On a smaller scale, a Privacy team may include their own Security specialist outside of the main Security team, or vice versa. The best reporting structures focus on bridging gaps and allow for critical insight and collaboration between Privacy and Security while simultaneously highlighting the value of each.

---

## Board Oversight of Privacy and Security Risk

The role of the board of directors/board of trustees is to provide risk governance and ultimately own Privacy and Security risk and oversight. Healthcare organizations have varying levels of enterprise risk management programs that allow the board to monitor key risks within the organization. Boards usually have expertise in key areas, such as finance, but more often lack cybersecurity and Privacy expertise, putting many at a disadvantage with the quickly shifting landscape and proliferating regulations. It has become increasingly evident that every board needs, at minimum, a robust foundation to adequately govern both Privacy and Security risk effectively. Much of this groundwork may only come from allowing Privacy and Security leaders the ability to share reports, insights, and candid opinions.

The board does not oversee the actual operations of the Privacy or Security Offices and they govern from a perspective of overarching strategy. In medium and large organizations, Security and Privacy may have a defined cadence of presentations in Audit or similar board committees, and a few may even have a dedicated cybersecurity committee. In smaller organizations, communication with the board by the designated Privacy or Security Officer may happen indirectly through a report that displays significant operational and risk metrics. Additionally, there are factors that can lead to the Privacy and Security leadership having no contact with the board. This can happen for the following reasons:

- The board and/or the enterprise risk management program isn't tracking or interested in security or privacy risk until there is a material breach;
- The Chief Privacy or Chief Information Security Officer may not have the background, expertise, or experience to make a suitable board-level report;
- Privacy or Security leader roles may be filled by a consultant with little to no visibility or access to the board; or,
- The report is being filtered through another person to the board, such as the Chief Executive Officer, who consistently attends the meeting. In this case, the messages are often not conveyed through a Security and Privacy lens, resulting in the opportunity for message distortion.

Regardless of the way the board chooses to engage, Privacy and Security have a unique opportunity to work together to develop board-level reports. One example report could focus on vendor risk management and can include combined metrics showing number of third party vendors with current access to PHI. This can be further expanded to show the numbers of contracts reviewed and vendors risk assessed by Privacy and Security per quarter with high level, relevant findings and shared remediation efforts. With this illustration, the board can be assured that Privacy and Security are focused together on lessening the effects of a third party cybersecurity incident with a data privacy impact of its entity patients. These types of integrated board reports can allow for a collective and inclusive message

about where potential impacts lie within the organization, the current and future projected landscape, how Privacy and Security actually fit together, and the enterprise planning to effectively manage the risks.

---

## Common Reporting Structures

- **Privacy and Security roles are fulfilled by the same person. The Chief Privacy Officer (CPO)/Chief Information Security Officer (CISO) are a single person.**

In a small or medium sized organization, limited resources may lead to Privacy and Security leadership roles being performed by the same person. Some large organizations may even have this structure, though it's far less frequent. For the right professional, this structure can work well given that communication and understanding are naturally facilitated. However, without effort, proper training, and support, Privacy or Security may be "treated as secondary," or even as a burden such as when both roles are assigned to someone who may also be tasked with other responsibilities (e.g., an office manager). This structure could allow organizations of any size to build privacy and compliance into IT products and services. While this allows Privacy and IT Security to maintain strong unification, if the leader is the CISO, it could create a gap in Privacy's inclusion in other organizational legal, regulatory and compliance functions or can make it appear to the enterprise that Privacy has less significance and less visibility. If the leader is the CPO, the same structural nuances could occur but may require Privacy leadership to have stronger than average technical knowledge and IT perspective. In this structure the combined Privacy and Security leader would likely have direct contact with the executive leader of the organization, but may not have access to members of a board of directors.

- **Both Privacy and Security report to the Chief Executive Officer, Chief Operating Officer, Chief Risk Officer, Chief Administrative Officer, or equivalent executive leader.**

In this scenario, the designated Privacy Officer and Security Officer roles are held by different people who both report directly to the Chief Executive Officer (CEO) or the equivalent top executive, such as the Chief Operating Officer (COO), Chief Risk Officer (CRO), or Chief Administrative Officer (CAO). This approach ensures that Privacy and Security are positioned at the highest level of the organization's leadership, emphasizing their critical importance. It also allows for streamlined communication and decision-making regarding Privacy and Security matters with a single executive leader. This is typically seen in small- to medium-sized organizations and one or both officers may also present at board meetings.

- **Privacy reports to the General Counsel and Security reports to the Chief Information Officer (CIO).**

Some organizations choose to have the Privacy Officer report to the general counsel or Chief Legal Officer while the Security Officer reports to the Chief Information Officer (CIO). This structure assumes that legal and regulatory considerations and information technology are distinct, but interconnected domains. The general counsel can provide legal and regulatory guidance related to Privacy, while the CIO can oversee technical aspects of Security. This is typically seen in medium to large size organizations. Again, one or both may also present at board meetings or the information may be funneled through the chief legal officer and/or chief information officer.

- **Privacy reports to the General Counsel, Security reports to the Chief Information Officer with further separation of duties within the IT Security team.**

Privacy remains a legal and regulatory focus in the Office of the General Counsel. This structure allows the entity to separate any potential conflict that may exist between operational, technical, strategic, legal, and compliance functions within the IT Security team. The Privacy, Legal, Audit, Governance, Risk, and Compliance technology functions report outside of IT Security, while the IT Security technical analysts and IT Security operations and access management remain under the IT Security Officer. While this provides additional technical focus to the functions in IT Security, it also can create a communication and functional gap between teams where the IT Legal, Risk, Audit, Compliance team(s) may not maintain visibility into IT projects, risks, and vulnerabilities that they would have when embedded directly within the IT Security team. This arrangement is less common and but could be seen in larger organizations with a global footprint. Board access can be limited to the general counsel and potentially the CIO.

- **In contrast to the example structure above, Privacy continues to report to the General Counsel and Security reports to the Chief Executive Officer, Chief Operating Officer, Chief Risk Officer, Chief Administrative Officer, or equivalent executive leader instead of the Chief Information Officer.**

This structure similarly allows the legal department to provide privacy guidance while allowing for the organizations to separate any conflict that the CIO may experience between information technology budget, business priorities, and security risks. While many CIOs can effectively balance these priorities as part of their duties, this separation from the CIO to a different executive business leader ensures that the IT Security functions (including IT Privacy, IT Legal, IT Risk, IT Audit and IT Compliance functions) are not negatively impacted by other IT operational, strategic and budget concerns. This appears more commonly in larger organizations and there can be less opportunity for Privacy or Security to have direct board contact.

- **Privacy and Security both report to Compliance.**

When both Privacy and Security are structurally accountable to the compliance officer, the enterprise develops a deeper understanding of the regulatory responsibilities. In some cases, these can be direct reporting relationships or dotted lines. While this allows Security to operate independently of IT operational priorities, it can however create a gap in Security's inclusion in IT functions and projects. Often it is the compliance officer providing reports at the board level. This structure may be seen across small, medium, or large organizations.

- **Cross-Organizational reporting with “dotted line” relationships.**

This structure helps to facilitate communications across organizations where an explicit cross-functional reporting structure does not exist. Privacy and Security may report to separate senior-most leaders; however, they maintain an official dotted line in reporting to each other’s leaders. This encourages communications between both, and facilitates alignment of priorities providing paths to escalate issues; however, this can be difficult for staff to potentially have two supervisors if there is a lack of collaboration amongst the leaders. This structure may be operational in any size entity, and there is also the least opportunity to have direct board connection.

*Regulatory Case: An entity website had an application failure. Logs were transferred to a vendor’s open and unencrypted server to assist with troubleshooting. The logs unknowingly contained regulated data which was made available to all the vendor’s customers and anyone else without an account. There were misunderstandings about the flow of data throughout the website, the types of data the logs contained, the security of the data transfer process, a lack of understanding of the vendor’s access management and cyber hygiene practices, and poor timing of communication among Privacy and Security about the incident.*

Regardless of the chosen reporting structure, what is important is that there be designated Privacy and designated Security officials with well-defined lines of communication and organizational leadership with other internal stakeholders and teams, business users, and customers. The important additional consideration is whether either or both Privacy and Security have the opportunity to maintain a direct line of communication with both the highest level of organizational leadership and with the board of directors/trustees. The concept that the board and C-Suite leaders are ultimately responsible for overseeing functions of the enterprise make it consequential for Privacy and Security to have a seat at the table to share the planning, preparation, and potential impacts first hand of each area.

Ultimately, there is no one-size-fits-all solution. The choice of reporting structure should align with the organization's goals and priorities. Structure will impact the organization at all levels. Regardless of the reporting hierarchy, it's crucial to ensure that the designated Privacy Officer and Security Officer have mutual respect for and direct access to one another and senior leadership. The Privacy and Security Officers are responsible, expected, and authorized to implement and enforce effective privacy and security governance strategies otherwise the enterprise bares the risk of patient safety and data protection issues. Organizational structure is just one of the challenges that can make it easier or harder.

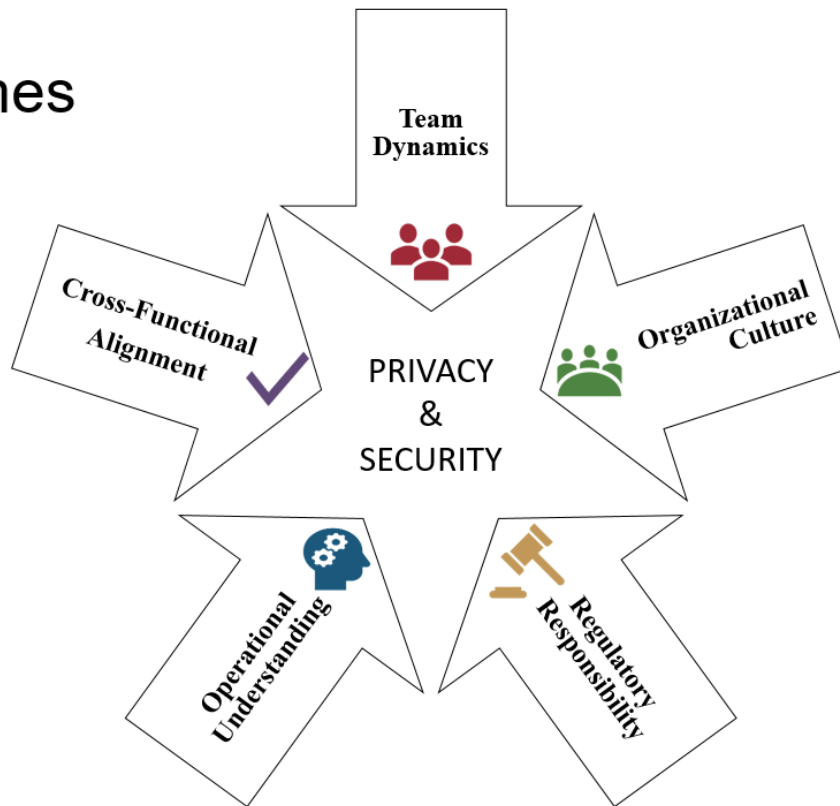
---

## Challenges between Privacy and Security and Organizational Risk

Depending on the size and complexity of the organization, Privacy and Security operational and strategic functions may be covered by a designated person, by separate teams consisting of any number and levels of staff and leadership positions, or hybrid combinations. Organizations should strive to have Privacy and Security operate in a unified manner since the end goal of patient, data, and system protection is largely the same. More often though, factors ranging from organizational structure to conflicting priorities can lead to disconnect between Privacy and Security, increasing organizational risk. The challenges arising from the separation and individualization of Privacy and Security roles, each with their own isolated strategies, can impact an organization in unanticipated ways.

Collaboration challenges fall into five overarching themes: (1) cross-functional alignment, (2) operational understanding, (3) team dynamics, (4) organizational culture, and (5) regulatory responsibility.

## 5 Themes



**Cross-functional alignment** denotes how Privacy and Security specifically coordinate efforts toward their common goals. It involves shared understanding of each other’s mission, goals, priorities, and areas of responsibility. This alignment requires a sense of accountability to, as well as collaboration with, the other area. Problems are likely to occur when there is undefined separation of duties, incomplete role coverage, lack of mutual goal setting, and/or a mission or vision that is unidentified or conflicting. Even divergent language can present challenges, obscuring a shared message across Privacy and Security. Weakness in operational or strategic unity presents issues with overall risk mitigation and acceptance.

*“Why do I have to complete two separate audits for Privacy and Security? They have the same types of questions, don’t your teams talk to each other?”*

*“Why did you choose to audit this vendor as high risk? Our team thoroughly audited them six months ago and they didn’t have any corrective actions.”*

**Operational understanding** implies Privacy and Security have day-to-day responsibilities *both* to the larger entity and to each other for efficient execution of tasks and monitoring of processes. Although Privacy and Security policies, procedures, and tasks may seem completely unrelated, foundational elements underlying them were likely drawn from concerns from both areas, and actions or decisions in one realm can significantly impact the other. Separation of duties without the accompanying deliberate effort to learn from each other can lead to unnuanced and

short-sighted decision making. Significant problems can develop in areas of technology adoption and/or implementation, especially in emerging areas such as artificial intelligence, if one group is slow to lead or is not adequately included in the necessary conversations. Poor operational understanding can lead to inadequate policies and procedures, insufficient documentation, and poor governance, which increases organizational risk. For example, regulated data is more than just protected health information (PHI) which may not be well understood by all in the organization. When PHI is misclassified, it can lead to misconfigurations in tools like data loss prevention (DLP) applications, resulting in unreported privacy incidents. Failure to adopt an industry-recognized framework, haphazard change management processes, and ineffective third party management can create inconsistencies in workflow especially in larger, more complex organizations. Keeping informed of the rapidly changing environment and addressing skillset gaps in Privacy or Security can reduce operational risks.

**Team dynamics** refers to interactions, relationships, collaborations, trust, and support between Privacy and Security teams within an entity. It is important for Privacy and Security to have respect for each other. Promoting consistent engagement of behavior and action from both teams requires active effort. Areas affecting Privacy and Security team dynamics are plentiful, can generate misalignment, and include: budgetary imbalance, unequal resourcing, or competition between leaders or teams. Inefficient and ineffective recruitment, onboarding, and retention lead to unpredictability and instability, forcing constant cycles where expectations and engagement are reset. Lack of trust is fragmenting and can lead to diminished achievements.

**Organizational culture** is the entity's overarching collection of values, attitudes, systems, and roles. This has direct impact on the effectiveness of Privacy and Security teams to accommodate aspects of business assurance. This often starts with the concepts of visibility, transparency, and acceptance from the top-down. The board and senior leaders must make a commitment to the principle that both Privacy and Security are valuable in their own right. Each has equally important roles to play in protecting the organization's interests, and therefore must understand when the other needs to be represented or informed within the larger organization. Symptoms of organizational culture issues can lead to: poorly coordinated qualification and quantification of metrics; lack of joint incident planning and management; absence of shared governance; redundant education initiatives; perceived or real hierarchies; and deficits in efforts toward institutional data mapping, flow, classification and minimization to broaden business processes and lessen risk.

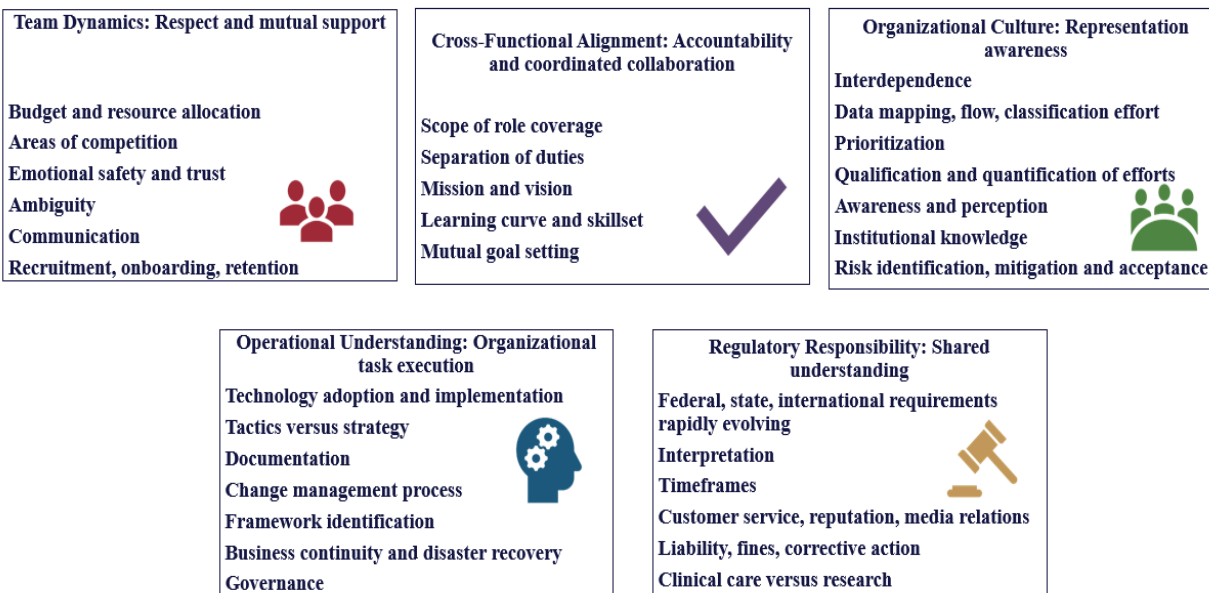
**Regulatory responsibility** is the duty to comply with all applicable laws and regulations for both Privacy and Security. This can include federal, state, and/or international requirements. Regulatory responsibility is one of the core duties of both Privacy and Security teams in the highly regulated and rapidly evolving healthcare sector. Shared governance is vital and should not just focus on the concepts of events, incident management, and breaches. Non-compliance with obligations surrounding reporting and the accompanying timeframes introduces risks of fines, corrective action, litigation, and reputational harm. Privacy and Security may identify different risks, speak different languages that lead to misunderstandings, or recognize different impacts. Situational assessments are not always comparable. As an example, a company may use a vendor to send out mass mailings. Security may identify the vendor's copy machine as being a potential vulnerability and Privacy may be concerned about incorrect mail merges on the documents being sent out.

*"I really wish the Security team would tell us right away when they have an incident. They never tell Privacy in a timely manner and we're always scrambling. We have strict regulatory timeframes."*

--



# 5 Themes



## Best Practice Strategies for Privacy and Security Interconnection

Challenges facing Privacy and Security can be interconnected. Suggested best practices for overcoming some of the specific problems include the following:

- Identify the current state
  - Document and recognize current capabilities and scope of duties for Security and Privacy.
  - Evaluate the effectiveness of each area. Identify the strengths, weaknesses, and gaps.
  - Jointly determine what the future state should look like for each area.
  - Determine how the areas should work together to support the goal of risk management for the organization.
- Prepare shared documentation and metrics
  - Create decision trees, flow diagrams, and/or a RACI matrix (see below for sample) to define the work being done and prepare for issues.
  - Create shared policies, procedures, guidance documents, and mechanisms for measuring effectiveness over time.
  - Make certain each are reviewers for the other’s policies.
  - Develop a comprehensive playbook with individual sections for Privacy and Security, with an additional joint section to address shared responsibilities.

*Consider what happens to cross references if Privacy or Security archives or removes a policy or the implications if language is inconsistent across policies.*



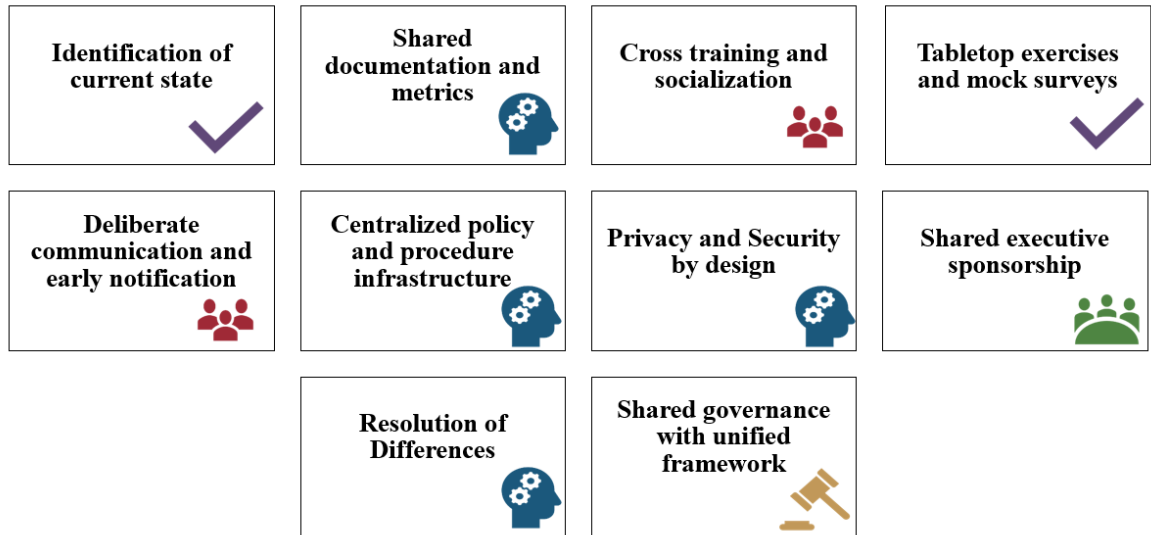
- Provide cross-training, education, and opportunities for socialization
  - Actively encourage joint Privacy and Security skill building to increase cross- functional knowledge of workflows, vocabulary, and topics of concern.
  - Collaboratively develop entity-wide staff education and materials to create a holistic approach to data Privacy and Security training.
  - Provide a trust environment to explore new ideas, ask questions, which can lead to enriched and more nuanced thinking in regular work activities.
  - Encourage relevant connections and socialization both within and outside of work-related activities helps to promote positive team dynamics.
  - Extend cross-disciplinary communication and training beyond the top level of each team in order to build workforce depth and prepare workforce members for growth opportunities.
- Conduct tabletop exercises and mock surveys
  - Consistently use tabletop exercises to provide the opportunity to understand successes, identify gaps, and more efficiently note where Privacy and Security can leverage each other’s expertise.
  - As an illustration, during a security incident a mitigation step taken could potentially result in erasure of evidence necessary for Privacy to effectuate a valid breach assessment.
  - Utilize simulations and planning to reduce stress in high-tension situations by adding elements of routine and familiarity.
- Build in processes for deliberate communication and early notification
  - Communicate. Communicate more. There cannot be too much communication.
  - Notify each other early to keep engagement between Privacy and Security high.
  - Identify situations and processes where communication between Privacy and Security need to be explicitly incorporated.
  - Be thoughtful, inclusive, and deliberate when developing mechanisms to ensure adequate coverage for Privacy and Security across the entire enterprise.
- Create a centralized policy and procedure infrastructure
  - Have a place where all Privacy and Security policies are kept and dually accessible.
  - Harmonize regulatory and legal responsibilities as much as possible.
  - For example, a shared understanding of the parameters for role based access allows Security to accurately provision access to sensitive information (social security numbers, credit card or other financial information, mental health or substance use information) based upon regulatory requirements noted by Privacy. This cuts down on access scope creep. It provides a way to scrutinize exception requests, determine in advance the approval levels required, and follow a documented and auditable process.
  - Cross-reference the other’s policies and procedures whenever possible.
  - Deliver education, policies, and procedures in an inclusive manner, irrespective of “ownership” boundaries.

*“How about we perform walkthroughs together? This way we can cover twice as much ground, educate each other on basic things to look for, and comprehensively mitigate issues we find. After the walkthroughs, let’s stop for lunch!”*

- Implement Privacy & Security by Design
  - Streamline the integration of controls and avoid last-minute complications by planning in advance.
  - Integrate Privacy and Security practices throughout the entire project/product life cycle.
  - Adopt technology and practices that address applicable regulatory requirements.
  - Incorporate the language and practices of Privacy and Security by Design as a framework to facilitate communication and collaboration.
- Identify shared executive sponsorship and support
  - Recognize the validity and impact of Privacy and Security as part of the culture of the organization
  - Promote the resourcing and budgeting of each area at the highest levels to show support of initiatives.
- Create a cross functional governance structure with a shared framework
  - Adopt common governance to promote transparency of decision making and accountability.
  - Use a shared framework to understand and manage risk through a collective format and language.
  - Align day-to-day tasks for Privacy and Security where possible to increase productivity.
  - Use shared applications and tools where possible to combine efforts.
    - Asset inventories or configuration management databases that contain information for both Privacy and Security allow for an understanding of company-wide data and systems.
- Create an appropriate setting and consistent opportunity to resolve differences
  - Keep lines of communication open to promote resolution of issues
  - Identify ways to settle conflicts and competing priorities through creative and mutually beneficial solutions.
  - Consider commonalities and differences in Privacy and Security interests to resolve issues as they arise.

*Regulatory Example: Both Privacy and Security should review and understand the regulatory risks of iframes, interactive content, embedded videos, plug-ins, etc. on websites because of unanticipated consequences of potential data leakage to third parties.*

# 10 Best Practices



## Use of Responsibility Assignment (RACI) Matrix

The use of a responsibility assignment matrix (**RACI**) is an example strategy of shared documentation that can be used to identify who is responsible (**R**), accountable (**A**), consulted (**C**), and informed (**I**) for tasks and decisions. The RACI template below provides a starting point for discussions of the current state and the desired future state of Privacy and Security in an organization. It offers flexibility and a roadmap to understand who is leading what areas and sets expectations up front. When there is occasion to review and agree upon expectations in advance, there is less chance of confusion when an actual incident occurs or when there is a new workforce member at any level in Privacy or Security.

For convenience, the template tool generally divides topics into Security, Privacy, and joint activities. It is meant to be customizable, promote discussion, and increase productivity. Some of the listed items are drawn from regulatory requirements (for example, the HIPAA Security Rule requires that an organization have a “Security official who is responsible for the development and implementation of [Security] policies and procedures.” 45 C.F.R. § 164.308(a)(2)). Items should not be removed without verification that they are out of scope for an organization.

*“Who needs to be involved in the process or exception allowance for regulated data to be accessed, exported, used, or disclosed offshore?”*

Users should modify and adapt it to meet their own desired practices and organizational setup. Smaller organizations can remove columns to utilize the template to identify key responsibilities of one person. Medium organizations may have combined or separated singularly designated Privacy and Security officers with or without a team. Larger organizations may have both individually designated Privacy and Security officers, typically with accompanying teams, and may require additional columns. Entities that must follow certain types of international regulations may also be required to designate a data protection officer. See example RACI template.

Organizations can fill out this template as a standalone activity, or the tool can be used prior to or during Privacy and Security tabletop exercises or mock surveys. It should be reviewed and revisited at a minimum annually, when Privacy or Security leaders change, and/or when the leadership structure changes. Users should feel permitted to allow Privacy or Security functions to be interchangeable or to be made collaborative/joint when it meets the needs of the actual business. By enhancing communication and shared understanding, efficiency is gained for the business.

## RACI Template



**R = Responsible**

**C = Consulted**

**A = Accountable**

**I = Informed**

Key Responsibilities	Designated Security Officer	Designated Privacy Officer	Data Protection Officer	Security Operations Team	Privacy Team
<b>Security</b>					
1. Ensuring compliance with the HIPAA Security Rule and other relevant Security regulations.					
1.1. Assessing current state and cultivating knowledge of existing environment and systems.					
1.2. Performing and overseeing Security risk assessment and management.					

<p><b>1.3. Ensuring the confidentiality, integrity, and availability of regulated/critical data and that systems are protected by the appropriate administrative, technical, and physical safeguards.</b></p>					
<p><b>1.3.1. Administrative Safeguards</b></p>					
<p><b>1.3.1.1. Developing, implementing, and enforcing policies and procedures associated with Security rules and regulations.</b></p>					
<p><b>1.3.1.2. Ensuring administration of required and appropriate cybersecurity training.</b></p>					
<p><b>1.3.1.3. Business Continuity/Disaster Recovery plan development and testing (within the scope of regulated or operational data availability or confidentiality needs).</b></p>					
<p><b>1.3.1.4. Evaluating (where appropriate, auditing) Security controls included in formal agreements with internal and external parties using regulated data (Data Use Agreement, Memorandum of Understanding, Minimum Security Standards, Security Addendum, etc.).</b></p>					

<p><b>1.3.1.5. Ensuring that necessary contracting elements, agreements, and protections executed and in place.</b></p>					
<p><b>1.3.1.6. Conducting internal Security reviews, audits, and assessments.</b></p>					
<p><b>1.3.1.7. Advising on Security-related matters involving data, especially regulated data.</b></p>					
<p><b>1.3.2. Technical Safeguards</b></p>					
<p><b>1.3.2.1. Ensuring that appropriate technical controls (encryption, firewalls, etc.) are properly implemented.</b></p>					
<p><b>1.3.2.2. Overseeing and auditing controls to ensure secure access/use of regulated/ critical data (e.g., role-based authorization occurs, inactive accounts are promptly terminated, user activity is properly logged, systems enforce password requirements, etc.).</b></p>					
<p><b>1.3.2.3. Overseeing integrity controls for regulated and critical data.</b></p>					

<b>1.3.3. Physical Safeguards</b>					
<b>1.3.3.1. Overseeing safeguards (locks, gates, doors, etc.) for devices and systems that have regulated/critical data (mobile devices, removable media, workstations, etc.).</b>					
<b>1.3.3.2. Overseeing safeguards for physical locations such as data centers where regulated/critical data and systems are stored.</b>					
<b>1.3.3.3. Reviewing other physical Security safeguards for which other entities are responsible/accountable but which directly or indirectly protect regulated/critical data (door locks, Security cameras, fire extinguishers, etc.).</b>					
<b>1.4. Security review for internal/external requests for use of regulated or organizational data.</b>					
<b>1.5. Overseeing/leading Security incident response.</b>					
<b>1.6. Supply chain risk management</b>					
<b>1.7. Other</b>					

# Privacy

<p><b>2. Ensuring compliance with the HIPAA Privacy Rule, Breach Notification Rule, and other relevant Privacy regulations.</b></p>					
<p><b>2.1. Ensuring the Privacy protection of all regulated and confidential data, including proper acquisition, use, and disclosure in any form or media, whether electronic, paper, or oral.</b></p>					
<p><b>2.2. Ensuring individuals' right of access and to control their data are protected.</b></p>					
<p><b>2.2.1. Ensuring a Notice of Privacy Practices is current, transparent, available, and consented when applicable.</b></p>					
<p><b>2.3. Performing and overseeing breach management or risk of compromise assessment.</b></p>					
<p><b>2.3.1. Ensuring the appropriate parties (agencies, patients, etc.) are notified in the event of a breach within the required timeframe.</b></p>					
<p><b>2.4. Ensuring administration of required and appropriate Privacy-based training.</b></p>					
<p><b>2.5. Developing, implementing, and enforcing policies and procedures associated with applicable Privacy rules and regulations (including for non-electronic data formats).</b></p>					



<p><b>2.5.1. Overseeing safeguards for regulated and confidential data in non-electronic formats (i.e., locked shredding bins, signs in waiting rooms/elevators about appropriate conversations, etc.).</b></p>					
<p><b>2.6. Overseeing and auditing controls and processes for ensuring appropriate acquisition, access, use, disclosure, and retention of regulated and confidential data (including criteria for role-based authorization, types of data, monitoring access activity, etc.).</b></p>					
<p><b>2.6.1. Issuing and managing (and, where appropriate, auditing) Business Associate Agreements, Data Use Agreements, Data Transfer Agreements, Standards Contractual Clauses, Binding Corporate Rules, etc.</b></p>					
<p><b>2.6.2. Setting minimum standards for permitted uses and disclosures of regulated and confidential data, including Limited Data Sets.</b></p>					
<p><b>2.6.2.1. Privacy review for internal/external requests for use of regulated or confidential data (Privacy Impact Assessment, Data Protection Impact Assessment, Legitimate Interest Assessment, Transfer Impact Assessment, etc.).</b></p>					

<p><b>2.6.2.2. Overseeing the issuance of and reviewing language changes to formal agreements with internal and external parties using regulated or confidential data (Data Use Agreements, Memorandums of Understanding, etc.), with a focus on the appropriateness of the request and the Privacy controls.</b></p>					
<p><b>2.6.2.3. Ensuring that case- specific Privacy requirements (e.g., use of regulated data for marketing, fundraising, research, public disclosure) are being met and are understood by the groups performing those functions.</b></p>					
<p><b>2.6.3. Overseeing safeguards (administrative, technical, and physical) to prevent intentional or unintentional use/disclosure of regulated data in violation of laws or regulations.</b></p>					
<p><b>2.7. Responding to Privacy concerns, complaints, suspected violations, issues, or reports.</b></p>					
<p><b>2.7.1. Overseeing the response to requests/complaints based on regulated patient rights (requests for amendment, accounting of disclosure, restriction, erasure, personal representatives, etc.).</b></p>					

<b>2.8. Overseeing Privacy incident response.</b>					
<b>2.9. Advising on other data Privacy related matters, such as those involving non-regulated confidential information.</b>					
<b>2.10. Conducting internal Privacy compliance reviews, audits, and assessments.</b>					
<b>2.11. Other</b>					
<b>Collaborative/Joint</b>					
<b>3. Ensuring compliance with regulatory requirements which fall jointly under both Privacy and Security, and/or where Privacy and Security collaboration is necessary for proper compliance.</b>					
<b>3.1. Ensuring patient, research subject, employee, and consumer rights are protected.</b>					
<b>3.2. Coordinating incident response.</b>					
<b>3.3. Coordinating and managing required and recommended training and awareness programs.</b>					
<b>3.4. Conducting audits and assessments (i.e., clinic walkthroughs, executed vendor agreement audits).</b>					
<b>3.5. Coordinating responses to regulators or auditors.</b>					
<b>3.6. Monitoring relevant changes to laws, regulations, requirements, and guidance, making changes to policies and procedures as appropriate, and communicating applicable changes to impacted parties.</b>					

<b>3.7. Ensure that appropriate sanctions are established and applied to workforce members who violate policies and procedures.</b>					
<b>3.8. Ensuring corrective action when partners fail to meet Privacy or Security obligations in contracts/agreements.</b>					
<b>3.9. Providing attestations and appropriate levels of detail about Privacy or Security controls for third parties (i.e., data custodians, data stewards, government auditors, business associates, data processors, etc.).</b>					
<b>3.10. Ensuring cybersecurity and Privacy laws and regulations are being uniformly followed.</b>					
<b>3.11. Other</b>					

---

### Organizational Structure Considerations for Privacy and Security

Thoughtful consideration by an enterprise for the Privacy and Security reporting structures can increase operational efficiency and decrease risk. A comfortable and well understood reporting relationship allows for Privacy and Security to maintain a functional alignment, have solid appreciation of the distinct operations of each area and where support is needed, present a unified and collaborative strategy, share knowledge to harmonize responsibilities for regulatory requirements, and maintain support from leadership and the board. The organizational structure sets a tone for the entire entity to follow and heads off potential conflicts. There is no correctly demarcated reporting relationship, but assessment of the pros and cons can encourage a proactive deliberation of where to support Privacy and Security as a part of the overall healthcare ecosystem. Each entity is encouraged to consider the pros and cons of its own organizational structure to determine and work toward optimal relationships between Privacy and Security.

The following is a table of the advantages and disadvantages of different reporting structures to be used as a guide. Entities are largely based on one of these structures: flat, divisional/departmental, product based, functional, or matrix. A flat structure implies there are very few levels between leaders and staff within the organization and is most often seen in small entities. A divisional structure happens when employees and leaders are aligned based upon the department or market served and not necessarily job roles. A product based structure centers around each individual manufactured good or service. Functional organizational structures often have multiple sets of teams with unique arrays of expertise. The largest organizations can have a matrixed model with each team reporting to multiple

leaders at the same time with many dotted-line or dual reporting structures. Each of these organizational types can impact the overall reporting relationships distinctively.

## Organizational Reporting Relationship Pros and Cons Table



Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
<p>Privacy and Security are the same individual person with the CISO/CPO as the single leader of both</p>		<ul style="list-style-type: none"> <li>• Single point of contact</li> <li>• Communication is built in</li> <li>• Streamlined strategy</li> <li>• Ease of embedding Privacy &amp; Security by Design</li> <li>• Cross-training and mentoring can easily happen</li> <li>• Ease of task coordination</li> <li>• Cost effective</li> <li>• May have the ability to have direct board access</li> </ul>	<ul style="list-style-type: none"> <li>• Limited resources</li> <li>• Operational priorities may lead to conflict or imbalance between roles</li> <li>• May be too much for one person to handle, especially if there are additional responsibilities</li> <li>• One area may take precedence over the other and either Privacy or Security can be devalued</li> <li>• Regulatory/legal compliance or IT operational functions can be overshadowed, misaligned, or misunderstood depending on if the CPO or CISO leads</li> </ul>	<ul style="list-style-type: none"> <li>• Small or medium organizations</li> <li>• Organizations where Privacy needs to be a key function built into a technology product or service</li> </ul>

Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
CEO, COO, CRO, CAO or similar senior leader		<ul style="list-style-type: none"> <li>• Privacy and Security have access to the highest level of leadership</li> <li>• Sets example for tone at the top governance</li> <li>• Streamlined communications</li> <li>• Optimized decision making</li> <li>• Direct knowledge of business strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Senior leader may not have the bandwidth to directly support or fully understand both roles as individual stakeholders</li> <li>• May not have ability to engage with board directly</li> </ul>	<ul style="list-style-type: none"> <li>• Small or medium organizations</li> <li>• Entities where Privacy and Security require additional emphasis and prioritization</li> </ul>
Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
Legal	IT (CIO)	<ul style="list-style-type: none"> <li>• Privacy has a strong regulatory focus and legal guidance is applicable</li> <li>• Security has a strong technical focus and allows better insight and oversight into technical configurations and other information system areas</li> </ul>	<ul style="list-style-type: none"> <li>• Requires active and deliberate communication to make certain Privacy understands technical and Security understands all regulatory and legal considerations</li> <li>• Opportunities for tasks to be unaccounted or differing priorities</li> <li>• Security tied to IT operations and priorities</li> <li>• Privacy may have conflict of interest within the Legal department</li> </ul>	<ul style="list-style-type: none"> <li>• Medium or Large organizations</li> <li>• Global entities</li> </ul>

Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
Legal	Another Senior Leader that is not IT (CEO, COO, CRO, or CAO)	<ul style="list-style-type: none"> <li>• Privacy has a strong regulatory focus and legal guidance is applicable</li> <li>• Security budget removed from IT operational and strategic priorities</li> <li>• Lower resource competition for Security</li> </ul>	<ul style="list-style-type: none"> <li>• Security may have less influence or line of sight into IT operations or strategy</li> <li>• Issues of cross-team communication and functionality can exist</li> <li>• Privacy may have conflict of interest within the Legal department</li> </ul>	<ul style="list-style-type: none"> <li>• Large organization</li> <li>• Organizations with significantly disparate IT responsibilities</li> </ul>
Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
Compliance	Part in Compliance, part in IT Operations	<ul style="list-style-type: none"> <li>• Having Privacy and Security compliance staff on the same team allows for deep understanding of the regulatory responsibilities in conjunction with both areas</li> <li>• Security compliance can serve as a liaison between Privacy and Security Operations</li> </ul>	<ul style="list-style-type: none"> <li>• Security staff who are external to the IT function may lead to exclusion or lack of visibility of projects or strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Large organizations with multiple teams of Security and Privacy staff on each</li> </ul>
Privacy Reports to:	Security Reports to:	Pros:	Cons:	Recommended for:
Cross- functional “dotted-line reporting” (Officially under Legal but also reporting to IT)	Cross functional “dotted-line reporting” (Officially under IT but also reporting to Legal or Compliance)	<ul style="list-style-type: none"> <li>• Multiple avenues for escalating issues</li> <li>• Encourages alignment of priorities between leaders</li> <li>• Formalization of complicated relationships can reinforce shared goals</li> <li>• Increased opportunities to build relationships</li> </ul>	<ul style="list-style-type: none"> <li>• May present confusion having separate leaders who may not share the same strategy or goals</li> <li>• Misaligned priorities across leaders can create complications</li> </ul>	<ul style="list-style-type: none"> <li>• Any organization where a formal reporting relationship between Privacy and Security is not otherwise established</li> </ul>

An accounting of the reporting structure should be taken within the larger context of any healthcare enterprise itself to also include the following additional considerations and it should be appraised on an ongoing basis:

- Size of entity (small, medium, large)
- Type of entity within the subsector (direct patient care, health plans and payers, emergency management, pharmaceuticals, laboratories, health technology, medical materials, public health, federal response and program offices, etc.) and can include profit versus not for profit
- Scope and scale business
- Financial outlook
- Potential for growth
- Overall business strategy
- Facilitation of resources both human and financial
- Privacy and Security leadership and staff current knowledge base and skill level(s)
- Span of control
- Complexity of enterprise
- Level of responsibility
- Authority level
- Role delineation
- Accountability
- Duplicate work
- Need for autonomy
- Aptitude to engage with business
- Verticals where Privacy and Security have maximum potential
- Capability to be agile and flexible in approach
- Ability for innovation and advancement
- Performance and success measures
- Sphere of influence
- Accessibility to board of directors/board of trustees
- Geography served
- Need for a separately designated Data Protection Official
- Regulatory responsibilities
- Market served of patients and other health care consumers
- Benchmarking of similar type entities

---

## Privacy Intersection with Security Practices

Frameworks, whether developed by public or private entities, are a key element to a mature Security program. Increasingly, the types and numbers of Privacy-specific frameworks are expanding. Rather than recreate existing work of both Security and Privacy frameworks, this guide highlights ways in which Security and Privacy can be brought together under these existing frameworks. Thus, refer to the [Health Industry Cyber Security Practices](#):



[Managing Threats and Protecting Patients \(HICP 2023 Edition\)](#) framework as an example of a starting point for a larger and more comprehensive discussion about organizational Privacy and Security structures.

---

## HICP

HICP outlines the top threats facing the Healthcare and Public Health Sector. Developed with every stakeholder in mind, organizations from small to large can benefit from the resources and best practices provided in the main document and additional two technical volumes. HICP aims to provide organizations with recommendations and best practices to prepare and fight against cybersecurity threats that can impact patient safety.

HICP was created jointly by the Health Sector Coordinating Council and the HHS 405(d) Program to raise awareness and grow cybersecurity practices to best position the health sector against the ongoing threats it faces. It offers 10 mitigating areas and suggested best practices that are widely recognized. Though focus is primarily Security-related, there are ways in which Privacy supports and enhances each of the general mitigation areas. Privacy personnel can benefit from HICP by learning about the cybersecurity threat landscape and some of the tools healthcare organizations use to face those threats. Understanding these in the context of one's own organization prepares the Privacy professional to collaborate more effectively with their Security colleagues.

These coordinated mitigation efforts are additional opportunities for there to be engagement between Privacy and Security toward shared goals. In particular, Privacy will likely have valuable contributions to the areas of:



- Organizational training and awareness efforts;
- Collective governance;
- Joint incident response;
- Third party risk management review and oversight; and
- Combined messaging to executive level and the board to effect support.




*“At the next board meeting, maybe we can give a five minute joint presentation with example of how Security risks can lead to Privacy incidents so they better understand the interplay.”*




These mutually beneficial tasks help increase the Security of the healthcare organization. Below please find some specific recommendations for ways in which Privacy can partner with Security to improve implementation of the HICP Mitigating Practices.

# Privacy Engagement with Health Industry Cybersecurity Practices (HICP)

## 10 Mitigating Practices

Mitigating Security Practice	Considerations
<p><b>Email Protection Systems</b></p> <p><i>The two most common phishing methods occur by email access: 1) Credential theft is where attackers leverage emails to conduct credential harvesting attacks on the organization. 2) Malware dropper attacks are used when attackers deliver malware through emails, which can compromise endpoints. An organization’s cybersecurity practices must address these two attack vectors. Because both attack types leverage email, email systems should be the focus for additional Security controls.</i></p>	<p><b>Email Protection Systems</b></p> <ul style="list-style-type: none"> <li>• Consolidate or enhance current education and overall awareness, especially in live training opportunities</li> <li>• Reinforce the elements of phishing training and be involved in the administrative support actions with leadership for those who repeatedly fail training</li> <li>• Combine policies and procedures for sanction and discipline, acceptable use of personal devices, electronic communication standards, regulatory response actions</li> <li>• Incorporate Privacy into Security exercises as part of the white team</li> </ul> 
<p><b>Endpoint Protection Systems</b></p> <p><i>An organization’s endpoints must be protected. Endpoints include desktops, laptops, mobile devices, and other connected hardware devices (e.g., printers, medical equipment). Because technology is highly mobile, computers are often connected to and disconnected from an organization’s network.</i></p>	<p><b>Endpoint Protection Systems</b></p> <ul style="list-style-type: none"> <li>• Incorporate device encryption into the training and awareness program particularly where a technical control is not automatically applied</li> <li>• Integrate data mapping and data flow efforts into the device inventory to create a comprehensive resource</li> <li>• Add technical requirements into Privacy policies and procedures to set expectations for remote operations, work from home, use of VPN, and use of personal devices</li> <li>• Cover endpoint controls in guidance documents and FAQs</li> </ul> 

<p><b>Identity and Access Management</b></p> <p><i>Health care organizations of all sizes need to clearly identify all users and maintain audit trails that monitor each user’s access to data, applications, systems, and endpoints. Just as you may use a name badge to identify yourself in the physical work environment, cybersecurity access management practices can help ensure that users are properly identified in the digital environment, as well.</i></p>	<p><b>Identity and Access Management</b></p> <ul style="list-style-type: none"> <li>• Determine together what allowable minimum access is for varying internal positions</li> <li>• Create a combined role-based access decision tree showing potential access levels for regulated data based on job functions</li> <li>• Coordinate policy development that allows for documented, repeatable, auditable procedures downstream</li> <li>• Allow Privacy to audit administrative areas (e.g., audits of terminated employees, employee oversight, or increased scope of access)</li> <li>• Identify software usage that may not be centrally managed for access permissions</li> <li>• Offer resource documents detailing how to correctly permission files, folders, shared drives, etc.</li> <li>• Be involved early in the incident response of access management-related Security incidents to review for potential Privacy concerns</li> </ul> 
<p><b>Data Protection and Loss Prevention</b></p> <p><i>A Security breach is the loss or exposure of sensitive data, including information relevant to the organization’s business and patient PHI. Impacts to the organization can be profound if data are corrupted, lost, or stolen.</i></p>	<p><b>Data Protection and Loss Prevention</b></p> <ul style="list-style-type: none"> <li>• Educate and train workforce to report any and all suspected events to either team as soon as possible</li> <li>• Ensure policies and procedures support incident notification, response, and breach assessment and reporting as a combined initiative</li> <li>• Share information related to data flow, data classification, and data mapping efforts for data protection</li> <li>• Support education on retention and destruction strategies</li> <li>• Coordinate on use of data loss prevention tool and other data guardian strategies</li> </ul> 
<p><b>IT Asset Management</b></p> <p><i>Organizations manage IT assets using processes referred to collectively as IT asset management (ITAM). ITAM is critical to ensuring that the appropriate cyber hygiene controls are maintained across all assets in your organization.</i></p>	<p><b>IT Asset Management</b></p> <ul style="list-style-type: none"> <li>• Reinforce the use of encryption and other basic cyber hygiene requirements, particularly in live training opportunities</li> <li>• Support governance for asset management and maintenance with workforce and leadership particularly around use of personal devices</li> <li>• Address incident management for lost or stolen device incidents</li> </ul> 

<p><b>Network Management</b></p> <p><i>Computers communicate with other computers through networks. These networks are connected wirelessly or via wired connections (e.g., network cables), and networks must be established before systems can interoperate. Networks that are established in an insecure manner increase an organization’s exposure to cyberattacks.</i></p>	<p><b>Network Management</b></p> <ul style="list-style-type: none"> <li>• Contribute to governance and rules that guide requirements for network segmentation to ensure medical devices and other critical devices are separated from guests’ devices and insecure networks</li> <li>• Advocate for network Security in situations with no IT representation to provide cross-representation</li> <li>• Form a partnership procedures for reviewing application programming interfaces (APIs), external integration requirements, or non-standard patient portal requests</li> <li>• Actively be a part of architecture reviews to advise about known data flows and corresponding legal requirements of regulated data</li> </ul> 
<p><b>Vulnerability Management</b></p> <p><i>Vulnerability management is the process used by organizations to detect technology flaws that hackers could exploit. This process uses a scanning capability, often provided by an EHR or IT support vendor, to proactively scan devices and systems in your organization.</i></p>	<p><b>Vulnerability Management</b></p> <ul style="list-style-type: none"> <li>• Address data protection within audit and monitoring plans, policies, and procedures for a vulnerability management program</li> <li>• Develop talking points to raise awareness within leadership of vulnerabilities and the need for resources to address</li> <li>• Review or audit patching schedules</li> <li>• Engage together in third-party risk management processes</li> </ul> <p>Perform an annual review of higher risk third parties, minimum standards, and/or medical device requirements</p> 
<p><b>Security Operations Center and Incident Response</b></p> <p><i>Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breach or loss. Incident response is often referred to as the standard “blocking and tackling” of information Security. Many types of Security incidents occur on a regular basis across organizations of all sizes. Two common Security incidents that affect organizations of all sizes are 1) the installation and detection of malware, and 2) phishing attacks that include malicious payloads (via attachments and links).</i></p>	<p><b>Security Operations Center and Incident Response</b></p> <ul style="list-style-type: none"> <li>• Communicate promptly with Security to allow synchronization of response when potential incidents are reported or discovered</li> <li>• Share intelligence</li> <li>• Collaborate on playbook development for incidents involving regulated or other confidential data</li> <li>• Share known data mapping and data flows that are available</li> <li>• Define who is leading in different areas of the incident management process prior to an event</li> <li>• Translate Security operations center events into contextual document of regulatory obligations</li> </ul> 

### Network Connected and Medical Device Security

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and are successful in the treatment of many diseases. As with all technologies, medical device benefits are accompanied by cybersecurity challenges. Cybersecurity vulnerabilities are introduced when medical devices are connected to a network or computer to process required updates, therefore in order to protect patients it is important to protect these devices. Medical devices are a specialized type of Internet of Things (IoT) device and rather than recreating cybersecurity practices for them, healthcare organizations are encouraged to extend the relevant cybersecurity practices from each of the other prescriptions, and implement them appropriately for medical device management.

### Network Connected and Medical Device Security

- Provide training and awareness to the workforce about risks of connected devices (cameras, SD cards, printers, medical devices, or other network connected devices)
- Support oversight of clinical engineering or biotechnical team plans throughout the organization
- Inform and relay guidance when auditing remote monitoring or performing data access reviews
- Cooperate in the development of policies, best practices, and risk management plans of digital innovations and emerging technologies
- Be involved in and support IT architecture and deployment reviews
- Support appropriate resourcing to leadership and the board
- Offer guidance on regulatory requirements
- Review contracts to assure regulated data and patients are protected.



### Cybersecurity Oversight and Governance

Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks. They set expectations and foster a consistent adoption of behaviors by your workforce. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

### Cybersecurity Oversight and Governance

- Unify as many policies and procedures as possible or utilize cross referencing to promote synergy
- Support and assist in training on acceptable use
- Support sanctions and discipline through the development of a consistent sanction policy and escalation grid that clearly communicates expectations
- Communicate joint oversight over the implementation and development of cybersecurity policies
- Establish a regular meeting cadence with members of Security to facilitate mutual education, strong relationships, and knowledge sharing
- Identify and analyze current cybersecurity challenges with the goal of coordinating risk management strategies
- Develop combined vendor risk assessment policies, procedures, processes, standards, guidelines, audits wherever possible
- Share knowledge of alternative frameworks for compliance, such as those according to the Department of Justice and Office of Inspector General
- Participate in and help scope the enterprise Security risk assessment and analysis
- Learn and understand basic Security operations and regulations to foster a consistent vernacular



---

## Crosswalks of NIST Frameworks

In 2020, NIST released a [Privacy Framework](#) that provides data protection strategies. The crosswalks between Privacy, Security, and Fair Information Practices Principles allow Privacy and Security a way to open discussion and more fully appreciate each individual area, identify gaps, and determine those where there is overlap. Combined risks can be addressed with more efficient resource utilization. It promotes the use of equivalent language when communicating messages of risk management within areas of data lifecycle management, identification, governance, protection, and shared controls. Privacy protections are directly related to information Security.

