



Health Sector Coordinating Council  
Cybersecurity Working Group



Manage  
Risks

Health Industry Cybersecurity

# Sector Mapping and Risk Toolkit (SMART)



OCTOBER 2025

---

## Table of Contents

About the Health Sector Coordinating Council Cybersecurity Working Group	5
Disclaimer	5
Foreword from the SMART Task Group Co-Chairs	5
To Provide Feedback	6
Sector Mapping and Artificial Intelligence	6
Executive Summary	7
What are Critical Functions?	7
What is systemic risk?	8
Why is identifying this type of risk important now?	9
Critical Functions and Cyber Risks	9
Building Resilience Through Critical Function Analysis: A Strategic Imperative	10
Why Network Effects Matter	10
The Pitfall of Reactive Responses	11
Resilience Over Reaction: The Role of CFA	11
From Fragility to Flexibility	11
Using the SMART Map Tool	11
<b>Phase 1: Risk Identification Process</b>	<b>11</b>
Step 1: Form a Collaborative Planning Team	13
Step 2: Create a Common Understanding of Materiality	13
Step 3: Determine Applicability of Critical Function Maps	15
Step 4: Customize the Prioritized Critical Function Maps	15
Step 5: Identification of Vendors and their Services/Products	15
Step 6: Conduct Critical Functional Analysis to Prioritize the Vendors	16
<b>Phase 2: Critical Vendor Mitigation</b>	<b>18</b>
Closing Summary	19

Appendix A – Critical Function Maps	20
<b>To Submit a Request for SMART Maps</b>	20
Map 1 Blood	21
Map 2 Claims and Payments	21
Map 3 Dialysis	22
Map 4 EMS	22
Map 5 Home Health	23
Map 6 Laboratories	23
Map 7 Medical Devices Manufacture and Distribution	24
Map 8 Medical Supplies Manufacture and Distribution	24
Map 9 Pharmaceutical Manufacture and Distribution	25
Map 10 Public Health Laboratory	25
Map 11 Public Health Strategic National Stockpile	26
Map 12 Public Health Surveillance	26
Map 13 Public Health Vaccines-Children	27
Map 14 Public Health Vaccines-Pandemic	27
Map 15 Radiology-Diagnostic	28
Map 16 Radiology-Therapeutic	28
Map 17 Retail Pharmacy	29
<hr/>	
Appendix B – Materiality	30
Inherent Risk Exposure Rubric Example	30
Control Environment Maturity Score Rubric Example	<b>Error! Bookmark not defined.</b>
Example Template	31
Heat Map Example	32
<hr/>	
Appendix C: Excel Template for Supplier and Services Critical Function Analysis	33
<hr/>	
Appendix D – Systemic Risk Governance Policy Template (including RACI diagram)	34
<hr/>	
Appendix E: Example Scenario	37
<hr/>	
Scenario	37
Phase 1: Risk Identification Process	38
Step 1: Build Collaborative Team	38
Step 2: Define Materiality	38

Step 3: Review all Critical Function Maps	40
Step 4: Customize the Prioritized Map	41
Step 5: Identify Vendors and their Services/Products	42
Step 6: Conduct Critical Function Analysis	42
Phase 2: Mitigations and Action Plans	44
<hr/>	
Glossary	45
<hr/>	
Acknowledgments	48
Co-Leads	48
Contributors	48

---

## About the Health Sector Coordinating Council Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) is a government-recognized critical infrastructure industry council of almost 500 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes free healthcare [cybersecurity leading practices](#) and policy recommendations, and produces outreach and communications programs emphasizing the imperative that ***cyber safety is patient safety***.

In April 2024, the CWG established the Sector Mapping and Risk Toolkit (SMART) Task Group consisting of more than 80 healthcare organizations, government and advisors to develop a way to visualize, identify and measure systemic risk posed by third party technology, software and communications services essential to clinical, administrative and manufacturing workflows. It is intended for use by all health sector organizations, including manufacturers, insurance providers, and healthcare providers of all sizes. The suggested best practices herein directly address Objective 10 in the [Health Industry Cybersecurity Strategic Plan 2024-2029](#) as well as recommendations from 2017 Health Care Industry Cybersecurity Task Force "Report on Improving Cybersecurity in the Healthcare Industry."

---

## Disclaimer

This document is provided for informational purposes only. Use of this document is neither required nor intended for compliance with federal, state, or local laws. Please note that the information presented may not be applicable to or appropriate for all health sector organizations. This document is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

The advice and template materials provided in this guide are neither intended nor offered as legal advice or legal opinions. HSCC-CWG and the authors are not practicing attorneys. This guide and the material herein are intended for educational and information purposes only. The reader should neither act nor fail to act on any legal matter based upon the information or advice provided in this document without first engaging a competent attorney licensed to practice law in their state or territory.

---

## Foreword from the SMART Task Group Co-Chairs

The critical functions in the health sector form a complex ecosystem of interdependent organizations of all sizes, including patient care, payment and data management systems, pharmaceutical, manufacturing, technology research, and public health administration. A cybersecurity event affecting a single supplier or third-party product that supports a critical function across healthcare poses one-to-many impact; i.e., disruption to a single payment clearinghouse can shut down a significant portion of the nation's healthcare delivery.

The impact of a cyber disruption on critical functions can include loss of patient data and payment information, theft of intellectual property, or exploitation of medical device vulnerabilities that lead to disruption of functionality or patient harm. The growth of ransomware threatens the availability of critical functions and systems, leaving organizations unable to provide services or products relied upon by patients and health professionals.

While larger organizations have dedicated resources to improve the resiliency of their critical functions, many small-to-medium sized organizations are lacking similar scale and need support with tools appropriate to their size, capability and resource constraints.

This document, the Health Industry Cybersecurity Sector Mapping and Risk Management Toolkit (HIC-SMART), is designed for leadership across the health industry regardless of organizational size. It provides actionable guidance and methods for managing systemic risks related to their Critical Functions and dependencies within the health system. Its goal is to empower these organizations to demand secure products and high-availability of services from their suppliers, thereby driving improved standards for Critical Functions across the entire healthcare ecosystem. In situations where customer leverage is insufficient to influence third party security, the SMART tool can help organizations anticipate potential incidents and develop backup and resiliency plans.

Health industry organizations are encouraged to:

- Coordinate adoption of this document with your: senior leaders; critical function process owners; information technology and cybersecurity teams; supply chain and business continuity functions; governance, risk and compliance management; and suppliers.
- Test critical workflow map templates found in [Appendix A](#) against your own enterprise profile to identify potential vulnerabilities and related risk. *Note: The maps in Appendix A are redacted to protect sensitive information that should be restricted only to those with a “need to use.” Original maps populated with specifically identified functions and services are available through a vetting process per the instructions appearing in the Executive Summary and introduction to Appendix A below.*
- Evaluate your Critical Function risk management programs against these SMART best practices.

## To Provide Feedback

The HSCC Cybersecurity Working Group intends to review and update this toolkit as experience and recommended improvements guide us. We encourage stakeholders who have implemented these risk mappings to provide feedback about its use and help contribute to an improved critical functions risk management program. Please send your comments at any time to: [Feedback@HealthSectorCouncil.org](mailto:Feedback@HealthSectorCouncil.org).

## Sector Mapping and Artificial Intelligence

As part of this work, this group did not consider AI as a separate component of the sector risk maps. For solutions, software, or applications that include AI, organizations can call these out as part of the mapping process. As of this writing the HSCC Cybersecurity Working Group is engaging several AI task groups to consider these third party and other risks to the sector. Those resulting publications will become available throughout 2026 and can be found at <https://healthsectorcouncil.org/hscce-publications/>.

---

## Executive Summary

Technology systems supporting the health sector are more complex and interconnected than ever before. Cyberattacks on third-party systems can result in cascading systemic impacts on clinical and administrative workflows. However, the complexity of the sector and sheer volume of third-parties (and fourth, fifth and n-th parties), make it very difficult for individual organizations to identify, assess, prioritize and mitigate systemic risk in their ecosystem.

This document provides methodologies for organizations to map healthcare systems in a way that enables identification of vulnerable chokepoints whose disruption could disrupt or sever the flow of electronic health information, payments, or medical services for core healthcare delivery and ancillary functions. By visualizing chokepoints in these workflows, organizations can measure their comparative risk in the system and focus investments and efforts on mitigating those risks.

In developing this toolkit, the SMART Task Group consisting of more than 80 healthcare organizations, government and advisors generated a list of core functions and services that underpin the health sector. Generalized workflows of those critical functions were then mapped, identifying general processes, organizations, data flows, IT systems, 3<sup>rd</sup> party systems – and potential chokepoints - that are critical for that workflow to be completed.

As stated above the maps that appear in this document are redacted. To access the substantive maps with specifically identified functions and services, please see [“To Submit a Request for SMART Maps”](#) in Appendix A.

### What are Critical Functions?

In healthcare, a critical function refers to essential services or processes that must continue without significant interruption to preserve life, prevent harm, and maintain the overall operation of the healthcare system. Critical functions in the health industry are performed by a complex ecosystem of interdependent organizations of all sizes spanning: patient care; payment and data management systems; pharmaceutical; technology research; manufacturing; and public health administration. These functions are indispensable for ensuring patient safety and effective care delivery, especially during emergencies or system disruptions. Critical functions must be maintained to prevent harm, preserve life, and ensure healthcare operational and administrative continuity. The process of managing the risks to critical functions is complex and requires ongoing monitoring and control.

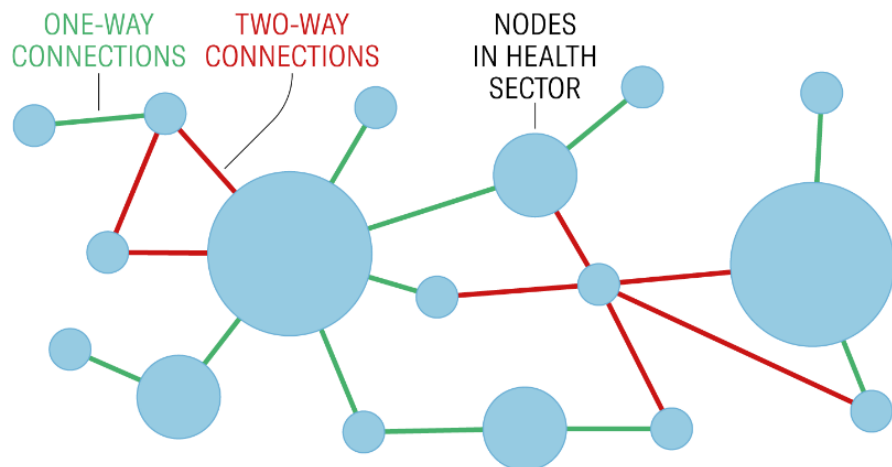
This document provides guidance to health providers and other health sector organizations for establishing a critical function risk management program. This involves: creating an inventory of clinical, business, and administrative business processes that support critical functions; documenting the associated workflows for the critical functions; identifying new and existing vendors, services, products, and technologies that enable the workflows; identifying and assessing the risk of each of the workflows; creating control and mitigation strategies to sustain those activities operationally; and validating and ensuring business continuity and resilience of all critical functions.

This document is structured to align with standard industry frameworks such as [National Institute of Standards and Technology’s Cyber Security Framework \(“NIST CSF”\)](#) and the [Health Industry Cybersecurity Practices \(“HICP”\)](#).

## What is systemic risk?

Systemic risk is the risk caused by interdependencies and linkages between parts of a system. When part(s) of the system fails, it causes a cascading failure that affects the entire system. As an example, the prevailing community assessment found that the Change Healthcare ransomware attack that occurred in 2024 exposed a systemic *concentration* risk in the healthcare sector. This attack compromised protected health information of at least 190 million people and disrupted the ability of hospitals, pharmacies, clinics, and medical practices that relied on Change Healthcare’s platforms to obtain pre-authorizations for procedures and payments for services rendered. This led to further downstream effects due to the interconnected nature of the healthcare ecosystem, including providers having to take out loans to keep their practices open; delays in treatments and patient care; and patients having to pay out of pocket for prescriptions and care, among other effects. These risks were largely unknown to organizations within the healthcare ecosystem prior to this event and almost all organizations had no mitigation plans to deal with downtime or disruption caused by this systemic risk.

**Figure 1 - Critical Function Risk and Materiality**



Source: Erik Decker et al.

HBR

*The circles represent nodes – or critical functions - in the sector. The size of each circle reflects the node’s “materiality” – how much the other nodes depend on it. Green lines represent one-way connections between nodes. Red lines represent two-way connections. The riskiness of both types depends on the nature of the data they exchange, the frequency of that exchange and the degree to which they have been secured. All things being equal, two-way connections tend to expose more risk than one-way connections. The more lines leading to a node and the greater its materiality, the greater the risks from cyberattacks it poses to the sector. From <https://hbr.org/2024/05/preventing-the-next-big-cyberattack-on-u-s-health-care>*

## Why is identifying this type of risk important now?

Over the last decade, the pace of technological innovation has continued to accelerate. To simplify workflow from the end user's perspective, the backend architecture has become more complex. Systems are integrated multiple times with multiple other systems to allow data to flow “seamlessly” between them, creating an ecosystem of interconnected systems that create, collect, transport, and store data. As new systems or devices are added, so are the numbers of interconnections and vulnerabilities. The ability of organizations to document and monitor these devices and systems, however, is inconsistent. According to the HSCC [Hospital Cyber Landscape Analysis](#), 91% of participating organizations monitor devices on their networks, yet only 52.6% of organizations have an inventory of *personal devices* on the network – a known class of exploitable vulnerabilities. With the proliferation of connected apps, APIs, and other tools that help move data into the hands of patients, the risk has also exploded.

The other driving force is the rise in third-party breaches. In a 2023 Ponemon Institute report, of the 47% of respondents who reported a ransomware attack, 46% stated it was caused by a third-party. The number of vendors that health organizations now do business with has continued to expand, increasing risk to those organizations. Additionally, the resources needed to vet those vendors and understand the risk in the relationship continue to increase. Widely disparate approaches across the healthcare sector for conducting third-party risk assessments create inefficiencies, costs and confusion among vendors who in effect are being asked to tailor their products and security controls to each of their many customers. The level of effort and resources needed to conduct and respond to third-party assessments often complicate the true purpose of conducting those assessments – to mitigate risk. The same 2023 Ponemon report found that only 49% of hospitals state that they have adequate coverage for managing risks to the supply chain. Therefore, not only is identifying the risks important, but doing it in a way so that resources can be deployed to mitigate the identified risks is what the health sector needs.

## Critical Functions and Cyber Risks

In the health industry, critical functions are essential services or processes that must continue without significant interruption to preserve life, prevent harm, and maintain the overall functioning of the healthcare ecosystem. These services support workflows within a healthcare delivery organization and often extend beyond the physical walls of a delivery location to encompass larger workflows across the health delivery system. Examples include manufacturing of supplies or pharmaceuticals, medical claims and payments, third-party pharmacy or laboratory operations, and emergency services. These functions are indispensable for ensuring that health care providers can deliver effective patient care and maintain financial liquidity, especially during emergencies. Any disruption to these functions can have severe consequences, directly impacting patient well-being and the ability of healthcare providers to deliver care. Patient care may be delayed or compromised, essential medications may not be dispensed, access to vital patient records could be lost, and emergency services could be disrupted, potentially increasing morbidity and mortality and/or loss of revenue leading to significant business impact.

Criminal groups and nation-state adversaries are able to exploit digital targets such as internet-connected devices, medical devices, legacy technology, cloud applications, third-party services, and the flow of suppliers within healthcare facilities. Exploits can take various paths, such as a supplier servicing an asset, poor manufacturer security design, vulnerabilities in installed networks, loaner/rental devices, manufacturer default passwords, and supplier applications interfaced into health systems.

The physical and digital supply chains play a vital role in supporting these critical functions by providing the necessary goods, services and data flows. However, the maturity of information security capabilities varies among suppliers, and historically the health industry has often relied on IT departments to manage cybersecurity risks independently of supply chain considerations. This approach is no longer sufficient.

Protecting critical functions in the health industry requires a proactive risk management strategy, especially within and across the supply chain. This approach is essential to safeguard patient information and other sensitive data such as trade secrets against growing threats from both external and internal actors. A robust risk management program is vital for enhancing preparedness, ensuring business continuity, and implementing effective countermeasures to protect critical functions. This is not solely an operational necessity but also a regulatory requirement. The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of patient information and the continuity of critical functions related to patient care. The U.S. Food and Drug Administration (FDA) enforces cybersecurity requirements and guidance aimed at securing medical devices and related technology.

Furthermore, Executive Orders [13636](#), [13800](#), and [14028](#) focus on enhancing cybersecurity for critical infrastructure and federal networks, emphasizing information sharing, developing cybersecurity frameworks, and modernizing IT infrastructure. These policies highlight the importance of collaboration between government and the private sector, and address issues like software supply chain integrity and the use of open-source software.

Finally, the “Identify” Core Function in the NIST Cybersecurity Framework recognizes the importance of identifying, mapping, protecting, and monitoring the workflows, roles, resources, suppliers and technologies supporting critical functions. Frameworks such as these provide a proactive approach for managing cybersecurity, risk, and supply chain management programs designed to protect continuity of operations within healthcare.

---

## Building Resilience Through Critical Function Analysis: A Strategic Imperative

In today’s interconnected operational landscape, network effects amplify both the value and the vulnerability of critical functions. A disruption in one vendor or their services/products can ripple across multiple departments, service lines, or even the entire organization — not because of the direct loss alone, but because of the interdependencies that bind systems, people, and processes together.

### Why Network Effects Matter

When a single vendor or their service/product fails, the impact is rarely isolated. Consider the following examples:

- A cloud-based EHR system going offline — affecting not just patient records, but billing, scheduling, and compliance reporting.
- A pharmaceutical supplier disruption — halting not only medication availability but also clinical workflows, patient throughput, and regulatory obligations.

These are network effects in action: the failure of one node destabilizes the entire system.

## The Pitfall of Reactive Responses

In the face of disruption, organizations often default to immediate tactical responses — rerouting services, shifting vendors, or pausing operations. While sometimes necessary, these actions:

- Are resource-intensive and often unsustainable;
- Can introduce new risks or compliance issues; and
- Do not address the underlying structural vulnerabilities.

Instead of relying on short-term fixes, organizations must proactively build resilience into their critical functions.

## Resilience Over Reaction: The Role of CFA

Critical Function Analysis is both a risk assessment tool and a resilience-building strategy. By simulating extended disruptions and evaluating the cascading impacts across the organization, CFA enables teams to:

- Identify chokepoints and concentrations of risk;
- Understand systemic dependencies and network vulnerabilities; and
- Develop sustainable mitigation strategies that are embedded into operations — not bolted on in crisis.

This approach ensures that when disruption occurs, the organization is not scrambling to respond; it is prepared to adapt.

## From Fragility to Flexibility

The goal of CFA is to shift the organization from a state of fragility where one failure can cause widespread breakdown to one of flexibility where systems are designed to absorb shocks, reroute intelligently, and recover with minimal disruption.

This is how resilience is built, not through improvisation but through intentional design.

---

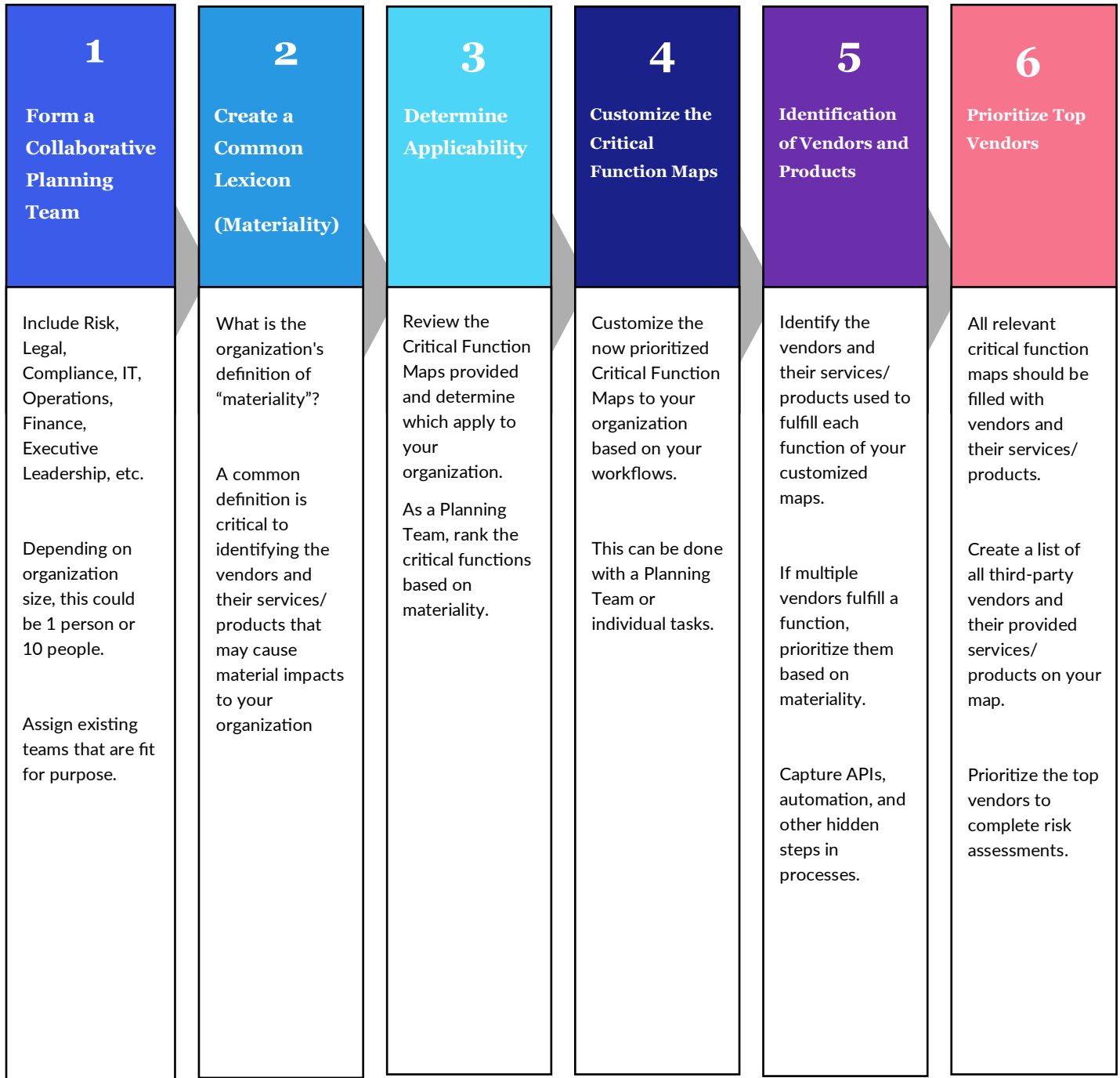
## Using the SMART Map Tool

The following two phases break down the process for filling in the *SMART* maps according to your organization's third-party service profile and then mitigating the identified risks to enhance resiliency.

### Phase 1: Risk Identification Process

Whether you're a rural hospital or Fortune 500 company, the pre-work necessary to identify third-party critical function risks remains relatively the same. The following diagram offers a step-by-step process for identifying an organization's essential vendors. Note that there is no set number of critical vendors as this is unique to each organization, but the number of critical vendors needs to be manageable, based on risk, materiality, and vendor tiering.

**Figure 2 – Risk Identification Process**



## Step 1: Form a Collaborative Planning Team

**Outcome: At the end of this step you will have created a team to work through Phase 1.**

The size and composition of your team depends on your organization, but the requirement for a cross-functional team is paramount. Determining your critical vendors cannot be done in silos based solely on the importance of one process, person or area of responsibility. Consider including the following areas, as applicable:

- Cybersecurity
- Enterprise Risk
- Legal/Privacy/Compliance/Internal Audit
- Information Technology/Operational Technology
- Clinical Engineering / Field Service
- Facilities/Physical Security
- Finance
- Executive/Clinical/Business Line
- Supply Chain
- Emergency Management/Business Resilience
- Other as necessary

For large organizations, planning teams may rely on sub-teams in individual departments that have specific subject matter expertise. These sub-teams may be stood up when specific workflows or critical functions are reviewed and assessed.

As governance is an important step in any organization, a policy outlining this work can be seen in Appendix D.

## Step 2: Create a Common Understanding of Materiality

**Outcome: At the end of this step, the team will have an agreed understanding of what materiality means to your organization.**

In healthcare, materiality often refers to the significance of a risk or disruption in terms of its potential impact on patient care, operational continuity, financial stability, and regulatory compliance.

Materiality is not universally defined; it varies based on the organization's size, structure, risk appetite, and stakeholder expectations. For example, a small clinic may consider a data breach affecting 100 patients as material, while a large hospital system might set a higher threshold.

When evaluating systemic risk - risk of disruption that can cascade across interconnected systems and vendors - materiality helps prioritize which functions, assets, or relationships require the most attention and resources.

Materiality is not just about size or cost, it's about criticality - how essential a function or vendor is to the organization's ability to deliver care and maintain operations. A material risk is one that, if realized, could cause widespread disruption, harm to patients, or regulatory violations.

Consider a few scenarios as materiality is assessed across several dimensions:

### **Clinical Criticality**

- Is the function essential to direct patient care (e.g., imaging, pharmacy systems)?
- Would its failure delay or compromise treatment?
- How would the clinical function respond to prolonged outage (5 days or more) as opposed to traditional response of minutes or hours of downtime?

### **Operational Dependency**

- Does the function support core operations like scheduling, billing, or supply chain?
- Is it tightly integrated with other systems?
- If the system becomes unavailable, what options are readily available to continue operational functionality for a prolonged outage?

### **Third-Party Risk Exposure**

- Is the critical function provided by a vendor or partner?
- What is the vendor's risk rating (e.g., cyber, privacy, resiliency)?
- If the system becomes unavailable, what options are readily available to continue operational functionality for a prolonged outage?

### **Recovery Complexity**

- How difficult is it to restore the function after an outage?
- Are exercised contingency plans in place to test outages for prolonged periods?
- What material systems should be considered that support the underlying services (e.g., active directory, single sign on, infrastructure)

### **Regulatory and Financial Impact**

- Could failure lead to significant fines, lawsuits, or reputational damage?
- Does it affect revenue cycles or compliance metrics?

Understanding your organization's definition of materiality is critical to planning, prioritizing, and executing response efforts for the systems that matter most to your organization.

### **Responsibility for Defining Materiality**

#### *Executive Leadership & Governance Bodies*

Ultimately, senior leadership (e.g., CEO, CFO, Chief Risk Officer) and boards of directors are responsible for setting materiality thresholds and ensuring alignment with strategic goals and regulatory requirements.

#### *Risk Management Teams*

These professionals conduct assessments, develop risk profiles, and recommend materiality thresholds based on data and organizational context.

### *Stakeholder Input*

Identify additional stakeholders to help avoid assumptions or over-classifying material systems. Input from patients, employees, regulators, and community members is crucial to identifying and contextualizing what is material from a broader perspective.

For more information on determining materiality, refer to [Appendix B](#).

### Step 3: Determine Applicability of Critical Function Maps

**Outcome: At the end of this step the team will have identified which of the critical function maps apply to your organization and will be analyzed.**

- Review the Critical Function Maps in Appendix A and identify which maps apply to your organization.
- Rank the critical function maps applicable to your organization. Complete steps 4-5 for each map selected; this serves as your starting point.

### Step 4: Customize the Prioritized Critical Function Maps

**Outcome: At the end of this step the team will have reviewed and updated the critical function maps to capture the details of your organization's specific workflows.**

- Review the map to ensure that it tracks your organization's workflow;
- Make adjustments where necessary by creating additional boxes and/or arrows to depict your specific processes. The SMART authors charged with creating the templates covered 80-90% of typical workflows; however, each organization may need to add, update and/or delete portions of the workflow, potentially in consultation with other related enterprise functions to capture accurately the exact process used;
- The workflow maps should be complete from start to finish and may need multiple reviews and iterations with subject matter experts (SME) in your organization.

### Step 5: Identification of Vendors and their Services/Products

**Outcome: At the end of this step, the team will identify all the vendors and their services/ products used within your critical function workflows.**

- Using the maps in Step 4, identify which vendors and their services/products your organization uses for each box and arrow of the critical function workflow. If there is more than one vendor/service/product, ensure that all are listed
- Capture all third-parties in the workflow, including APIs, automations, and other steps which may be hidden in the process. Consult with your SMEs to ensure that all vendors/services/products are identified.
- Identify risky and protected connections (e.g., full bi-directional network connectivity or limited privileged access and control across external organizational networks).
- Repeat this process for ALL relevant Critical Function Maps.

## Step 6: Conduct Critical Functional Analysis to Prioritize the Vendors

**Outcome: At the end of this step, the team will have a prioritized list of vendors including those whose services/products require additional risk mitigation.**

Once critical functions, vendors, and workflows have been identified in steps 4 and 5 the next step is to conduct a Critical Function Analysis, often referred to as “workshop”, to assess the resilience of each function and its dependencies. This process simulates a severe disruption scenario and guides the organization toward identifying chokepoints and concentrations of risk.

### **Step-by-Step CFA Process**

#### **1. Start with the Critical Function Map**

- Use the list of vendors/services/products and the critical function map developed in Step 5.
- Select one vendor/service/product at a time and apply steps 2–6 before moving to the next.

#### **2. Apply a Standardized Disruption Scenario**

For each vendor/service/product, assume the following test case:

- The vendor/service/product has been compromised and is completely unavailable.
- Notification of the disruption is received on a Friday at 4:00 PM.
- No estimated recovery time is provided; assume downtime will last weeks to months.
- Contractual remedies are unenforceable.
- No external aid (federal, state, or local) is available.

This scenario sets a worst-case baseline for evaluating resilience.

#### **3. Facilitate a Cross-Functional Impact Assessment (see [Appendix C](#) for a possible template to document this work)**

Engage a cross-functional team to answer the following:

##### *a. Operational Impact*

- How is the critical function affected?
- What processes or operations can and cannot continue?
- What are the short-term and long-term consequences?
- How long can the organization operate under this particular disruption?

##### *b. Existing Mitigations*

- Are there built-in alternatives or workarounds?
- How effective are these mitigations under the assumed scenario?

*c. Scope of Material Impact*

- Is the impact isolated to a single service line or vertical?
- Does it affect multiple service lines?
- Is it material to the entire organization?

**4. Identify Chokepoints and Risk Concentrations**

- If the vendor/service/product is deemed material to the business, add it to the list of chokepoints or concentrations of risk.
- This list will inform Phase 2 of the risk management program.

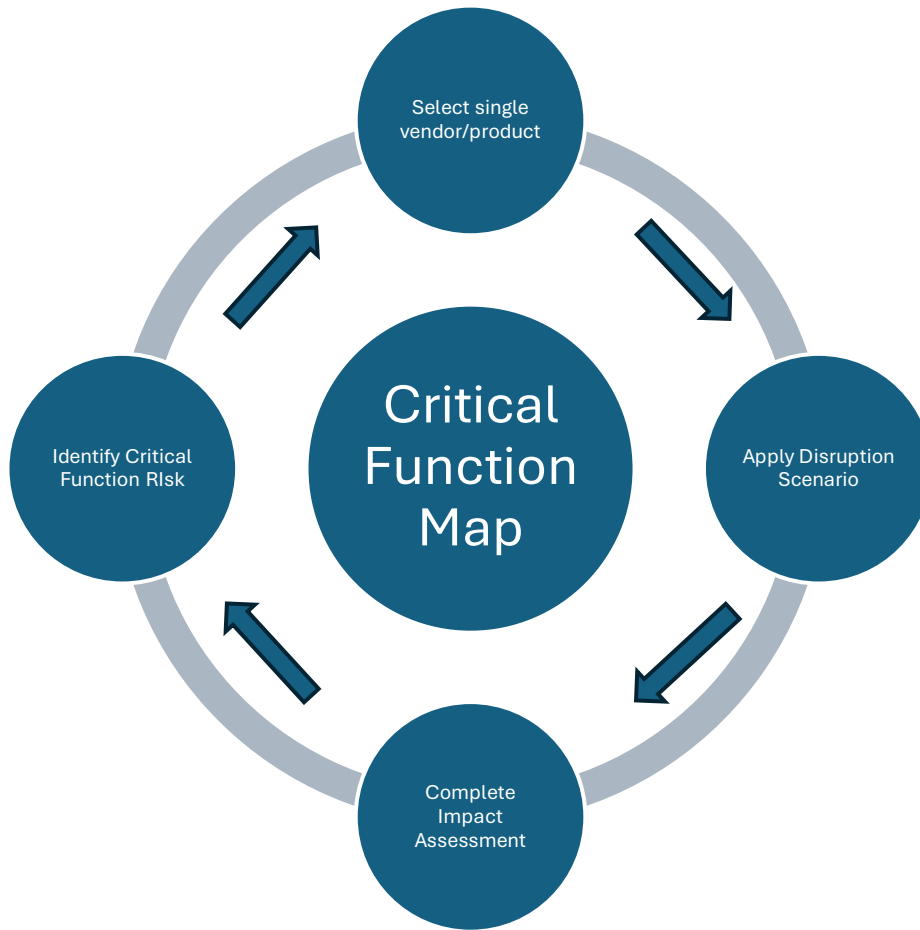
**5. Repeat for All Vendors/Service/Products**

- Return to Step 1 and repeat the process for the next vendor/service/product.
- Once all vendors for the current function are assessed, move to the next critical function map.
- Continue until all critical functions have been analyzed.

**6. Compile and Transition to Phase 2**

- The final output is a comprehensive list of material vendors/service/products.
- This list becomes the input for Phase 2, where deeper risk mitigation strategies are developed.

**Figure 3 - Diagram of step-by-step critical function analysis process**



## Phase 2: Critical Vendor Mitigation

**Outcome: Create management plans to mitigate identified material risk.**

Organizations should follow a comprehensive process to conduct thorough risk assessments for critical vendors. This process starts the same for a critical vendor as it does for one of low risk and involves several key steps and collaboration between various teams to ensure that risks are identified, managed, and mitigated effectively.

### **Initial Request and Questionnaire**

The process begins when a business owner requests a risk assessment. The vendor is required to fill out a detailed questionnaire that covers various aspects of their security posture, control adherence, and data protection measures.

### **Review and Documentation**

A Risk Assessor reviews the completed questionnaire and documents any findings or risk concerns. This includes identifying areas where the vendor needs to improve and informing the vendor for corrective action.

This process may include discussions with the vendor team regarding their questionnaire responses and/or their proposed implementation architecture, technical and operational risk concerns, and backup and recovery plans. However, when making vendor calls, prioritize vendors considering scalability for small and medium sized organizations with many vendors.

### **Vendor Tiering and Criticality:**

Vendors are tiered based on their business criticality and the amount of Protected Health Information (PHI) they handle. Critical vendors undergo more frequent and detailed assessments, while lower-tier vendors are reassessed less frequently.

Vendor Tiering also allows stratification of requirements for contracting, including different contract terms (e.g. right to audit, service level agreements, etc.) and different effort for monitoring vendor performance to those contract requirements. This also helps organizations scale workloads.

### **Standardization and Workflow:**

The organization should standardize the workflows for risk assessments to ensure consistency and clarity. This includes defining what needs to be documented and where, as well as setting expectations for the assessment process.

### **Action Plan and Follow-Up:**

The Risk Assessor/Team develops action plans to address any identified risks. When developing plans, identify risks not only associated with the platform/tool/software being implemented, but also any risks with the core infrastructure required to support the platform/tool/software.

These plans are tracked and monitored to ensure timely completion. For high-priority tasks, evidence of completion is required, while for medium and low-priority tasks, documenting the plan to address the issue is sufficient.

### **Escalation and Communication:**

If a vendor is unresponsive or fails to address the findings, the issue is escalated to higher management for further action. Communication with vendors may be facilitated through specialized commercial tools which can help streamline the process and improve response times.

---

## **Closing Summary**

Healthcare is an industry that requires preparation to enable appropriate response in times of need. As healthcare continues to experience highly impactful and prolonged outages, largely due to ransomware, this requires organizations to prepare to analyze its vulnerabilities in detail and take proactive measures to prevent future attacks.

By forming collaborative planning teams, creating common lexicons, and customizing critical function maps, organizations can effectively identify and prioritize their critical vendors and products. The document emphasizes the importance of understanding materiality, conducting thorough risk assessments, and developing robust mitigation strategies to ensure the resilience of critical functions. By following the outlined steps and leveraging the provided templates, organizations can enhance their preparedness, ensure business continuity, and safeguard patient care and safety. Using this defined process can help organizations focus on remediating risks from prioritized

high-risk vendors found during risk assessments, instead of just conducting numerous risk assessments and assuming all vendor risk is equal. This proactive approach to risk management is essential for maintaining the integrity and availability of critical functions in the ever-evolving healthcare landscape.

To integrate and contextualize the various tasks discussed in this guide, refer to [Appendix E for an example scenario](#) that can illustrate your enterprise interconnections, materiality and decision analysis.

---

## Appendix A – Critical Function Maps

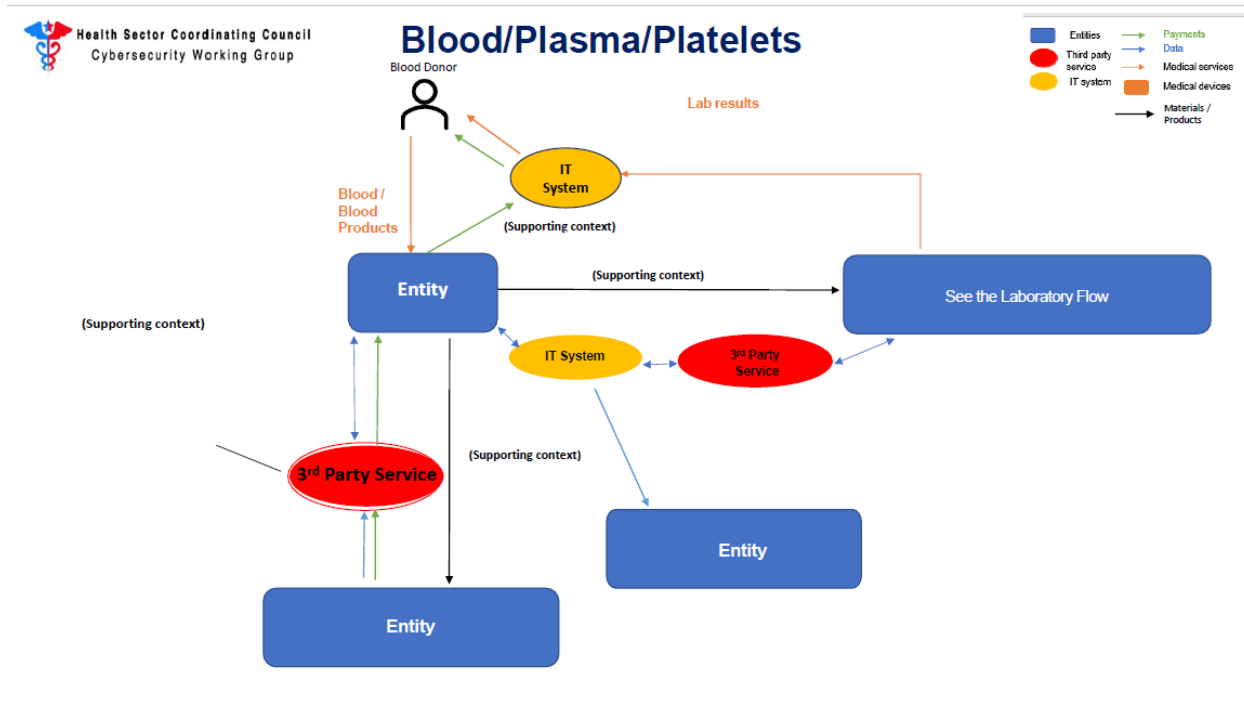
The HSCC SMART Task Group determined that the information presented in the completed systemic risk maps is sufficiently sensitive and revealing as roadmaps for adversarial disruption that we should not openly distribute the maps without an appropriate gating mechanism that restricts the sharing only with organizations that can demonstrate a “need to use.” The process for HSCC members and qualified non-member stakeholders to request the fully populated maps is discussed further below. The process was designed to be as low-friction as possible to ensure widest possible distribution to and usage by qualified healthcare organizations.

For general illustration purposes, sanitized versions of the 17 sector risk maps are included in the following pages and redacted to replace named types or functions of critical “Entities”, “IT Systems” and “Third Party Services” that are referenced in the legend of each map with only those generic terms in the legend. For example, an “IT System” could be an EMS; an “Entity” could be a “Health Provider” and a “Third Party Service” could be “Coding and Billing.” We present these maps to both privileged users and public “non-users” for the purpose of visualizing and appreciating the complexity of health systems and the difficulty of undertaking an effective program of risk identification, measurement and prioritization, and management.

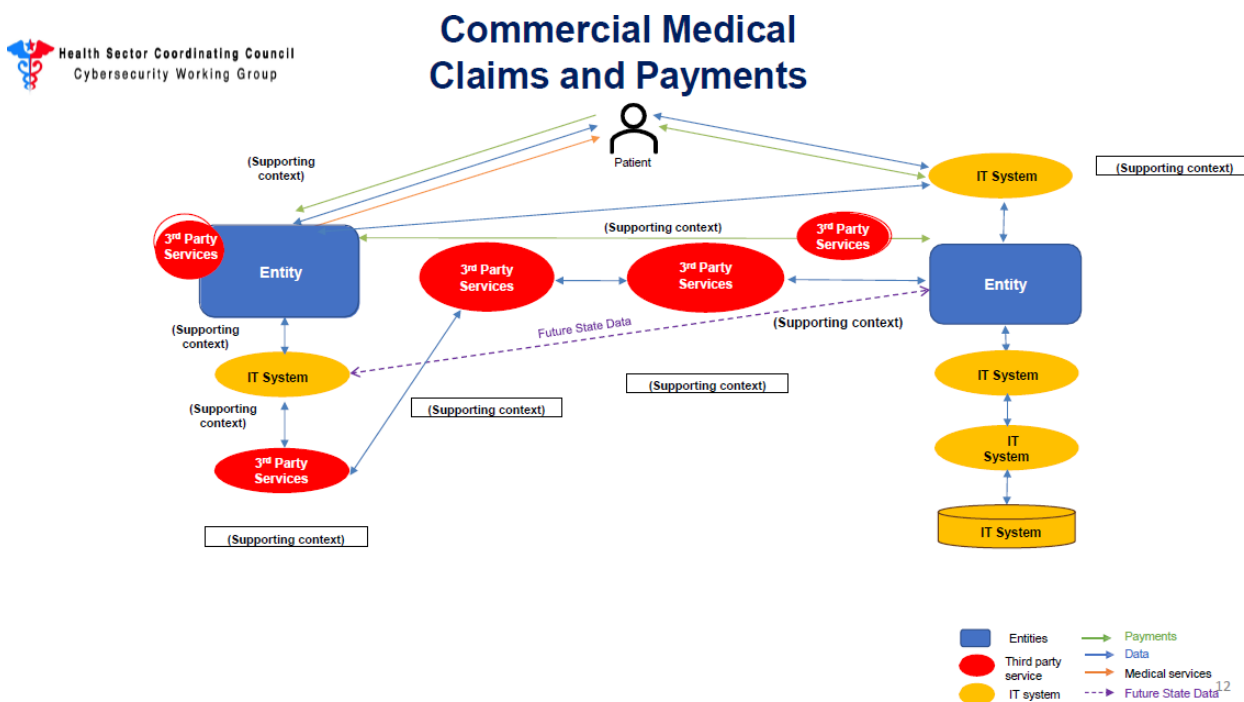
### To Submit a Request for SMART Maps

- Requestors are asked to go to <https://healthsectorcouncil.org/workflow-maps-request> to request the workflow map(s) you need.
- Requestors will be asked your name, title, organization, website, and email address, and which specific maps you need. This is to validate users to protect sensitive material and restrict its distribution on a “need to use” basis. Accordingly, requestors must represent legitimate health sector entities or core support functions (i.e., no Gmail, Yahoo, Hotmail, or other non-specific domains). Maps are marked “**Traffic-Light Protocol Red**” meaning they must not be shared outside of your organization.
- Requests will be vetted to restrict access for only those organizations with a “need to use”; i.e., regulated healthcare entities and essential infrastructure service providers and consultancies that support these work flows. Members of the press are not eligible to receive the workflow maps other than what is included in Appendix A.
- Requestors will be asked if you are willing to share lessons learned or improvements at a later date for subsequent maps in an iterative process. This is not required.
- Upon approval, a link to the requested map(s) will be delivered in a timely way.

## Map 1 Blood

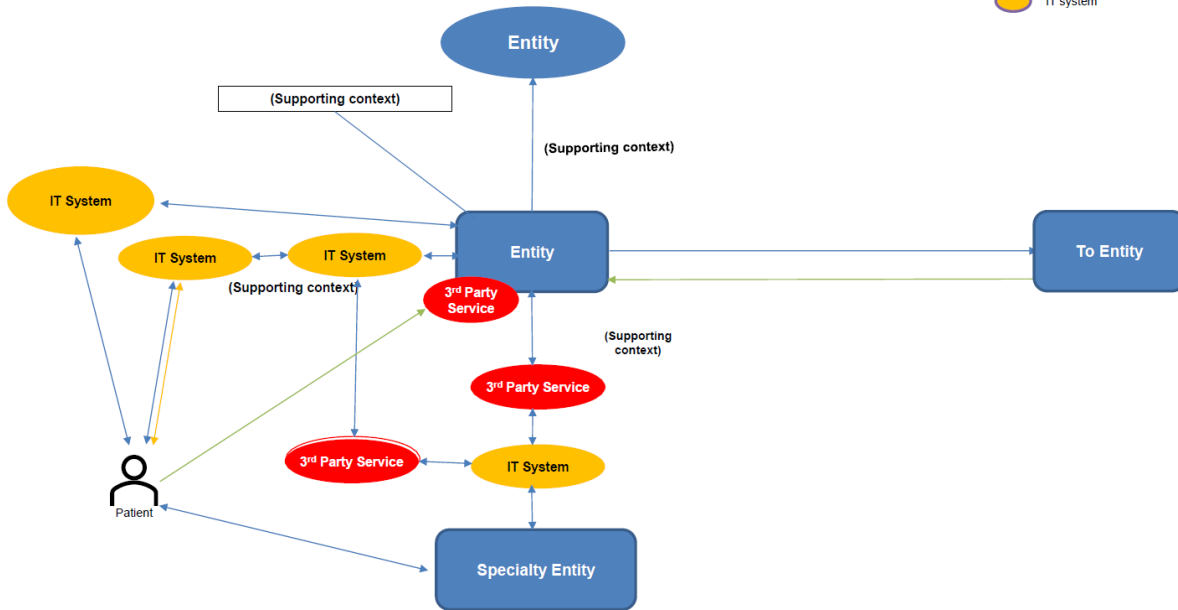


## Map 2 Claims and Payments

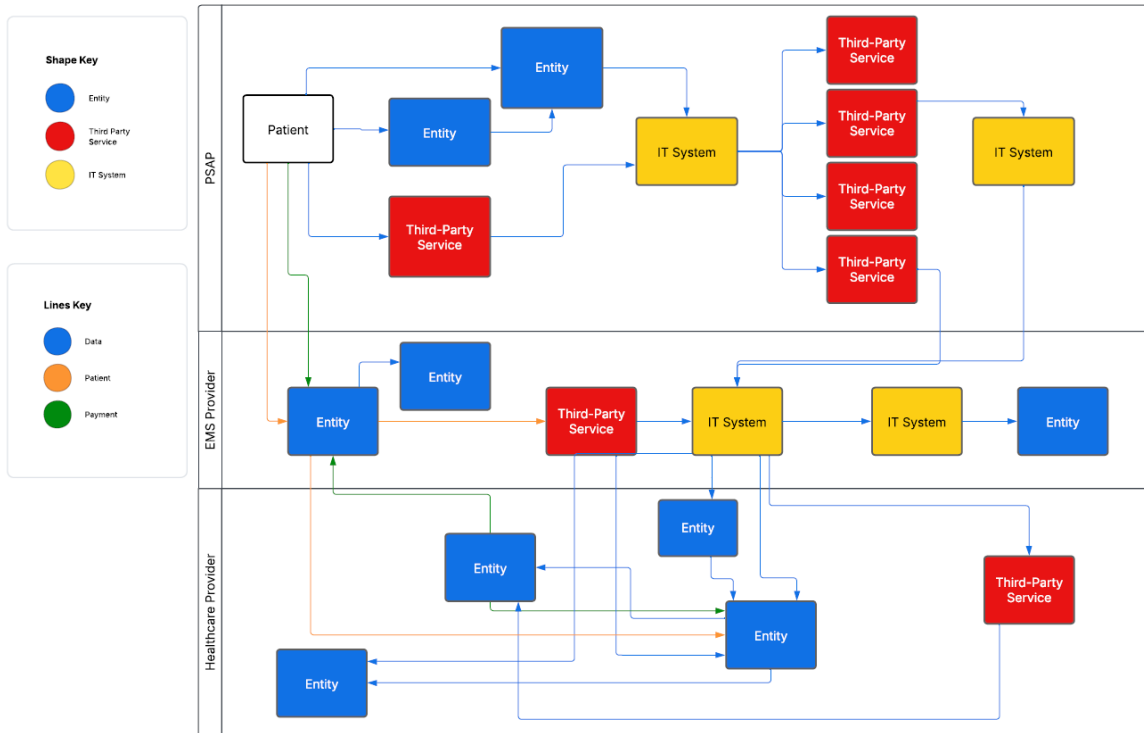


### Map 3 Dialysis

## Outpatient Dialysis



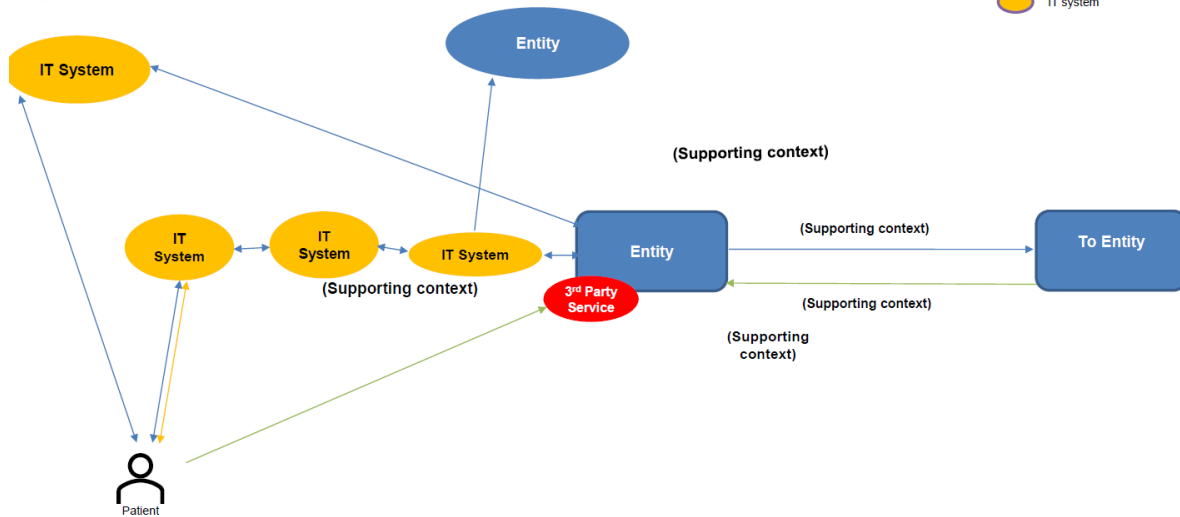
### Map 4 EMS



## Map 5 Home Health

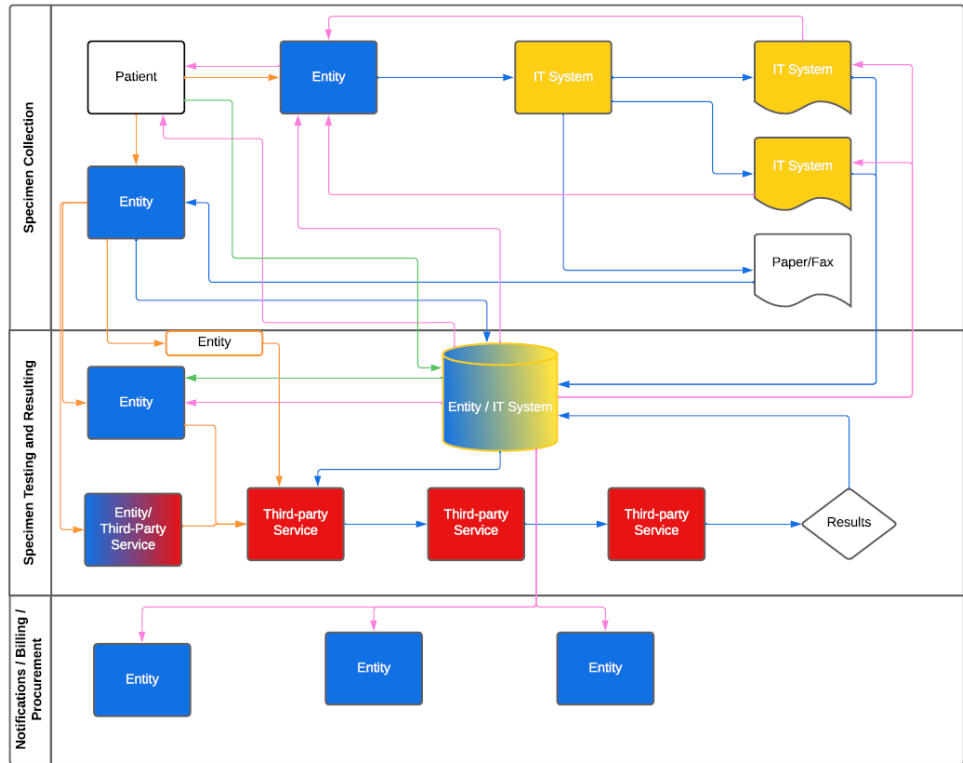
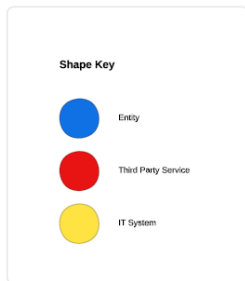


# Home Health

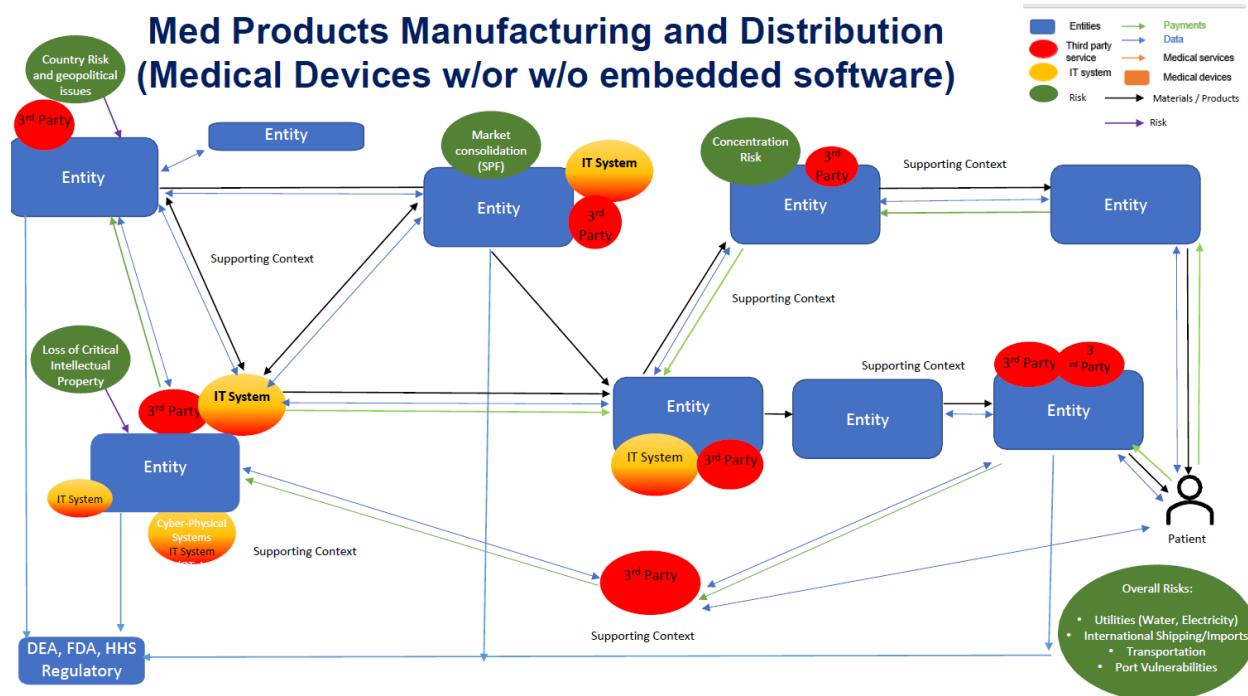


## Map 6 Laboratories

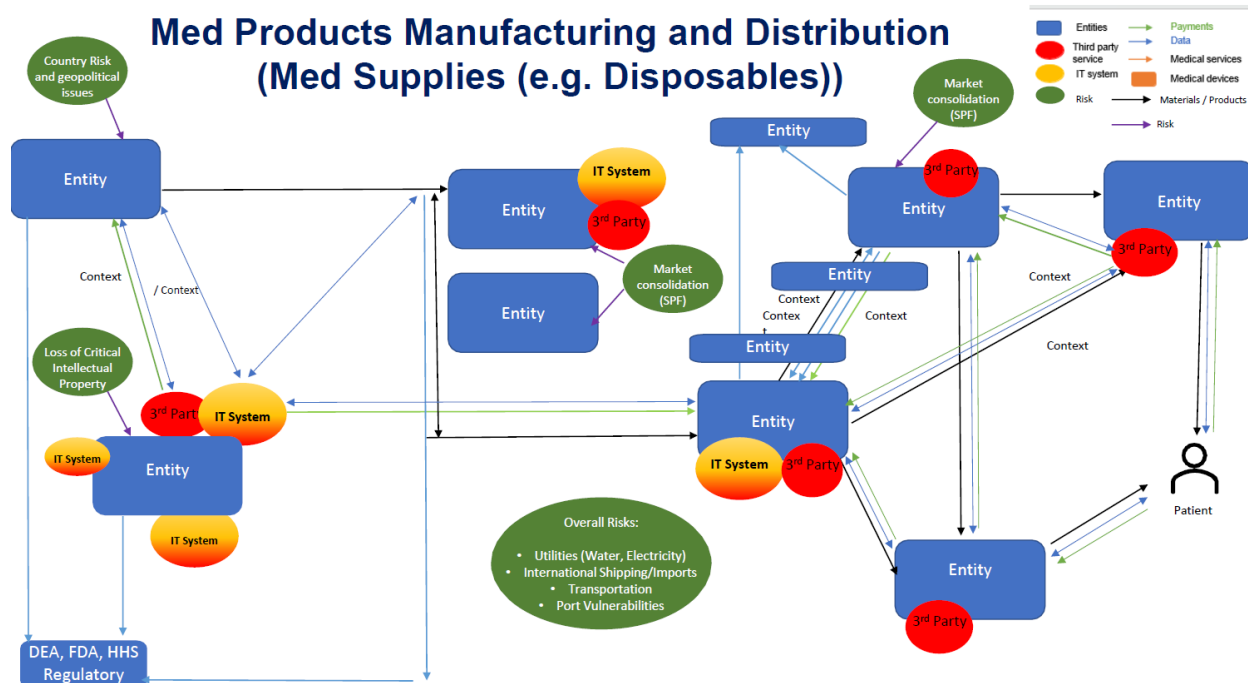
### LABORATORIES MAP



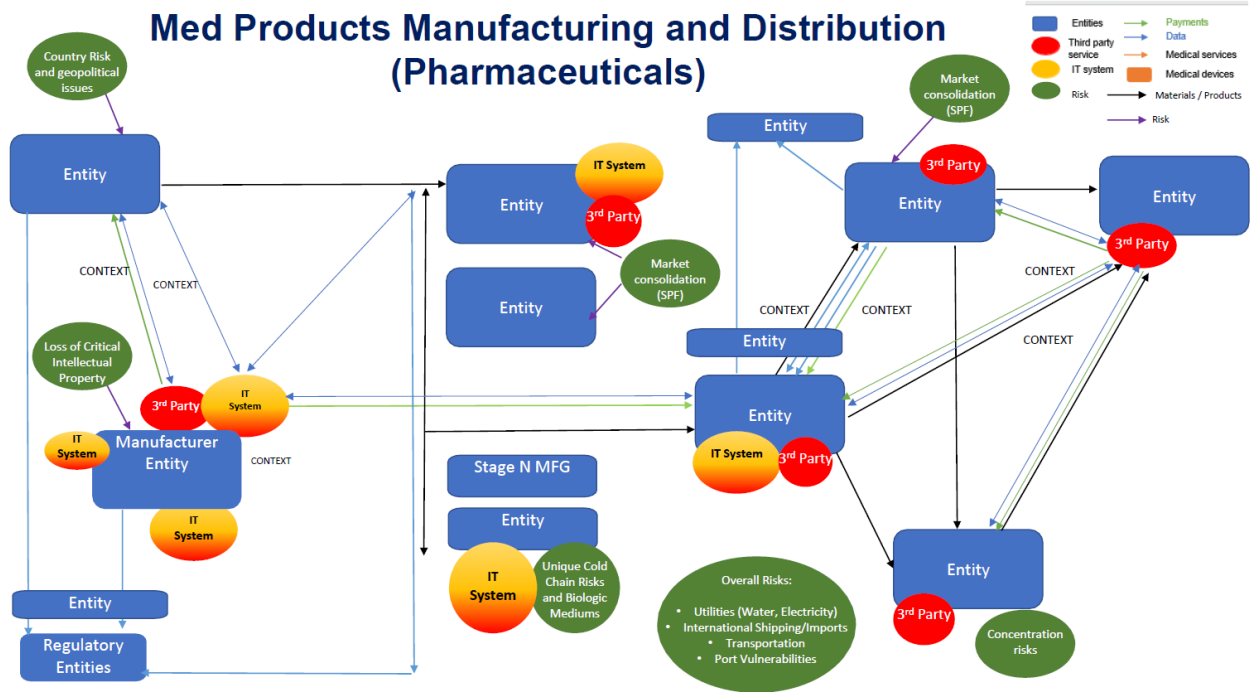
Map 7 Medical Devices Manufacture and Distribution



Map 8 Medical Supplies Manufacture and Distribution

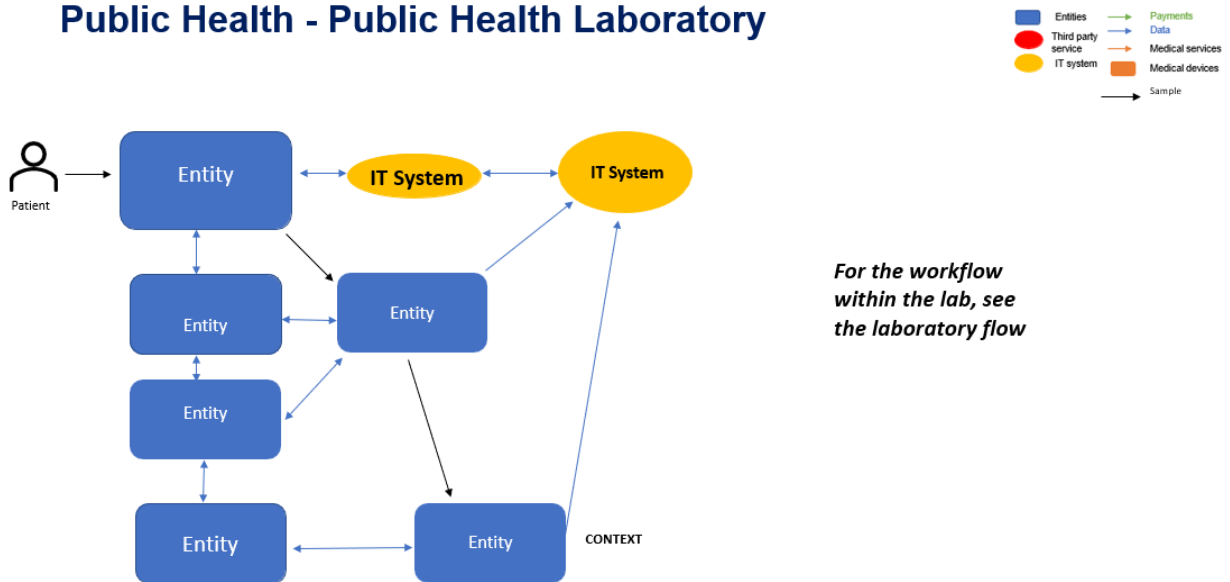


## Map 9 Pharmaceutical Manufacture and Distribution



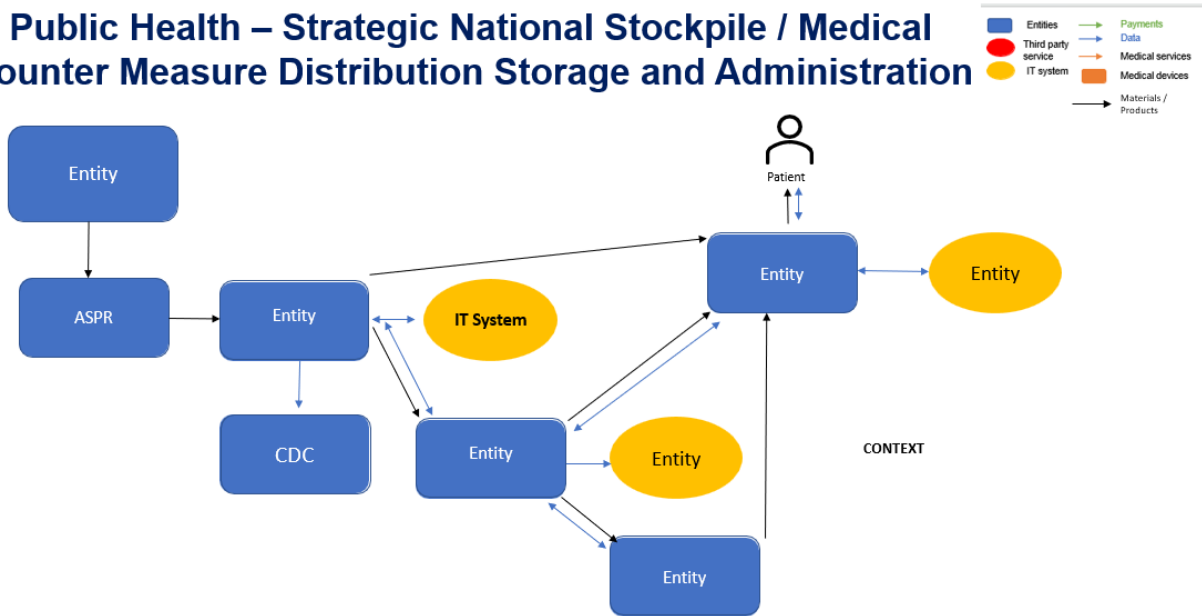
## Map 10 Public Health Laboratory

### Public Health - Public Health Laboratory



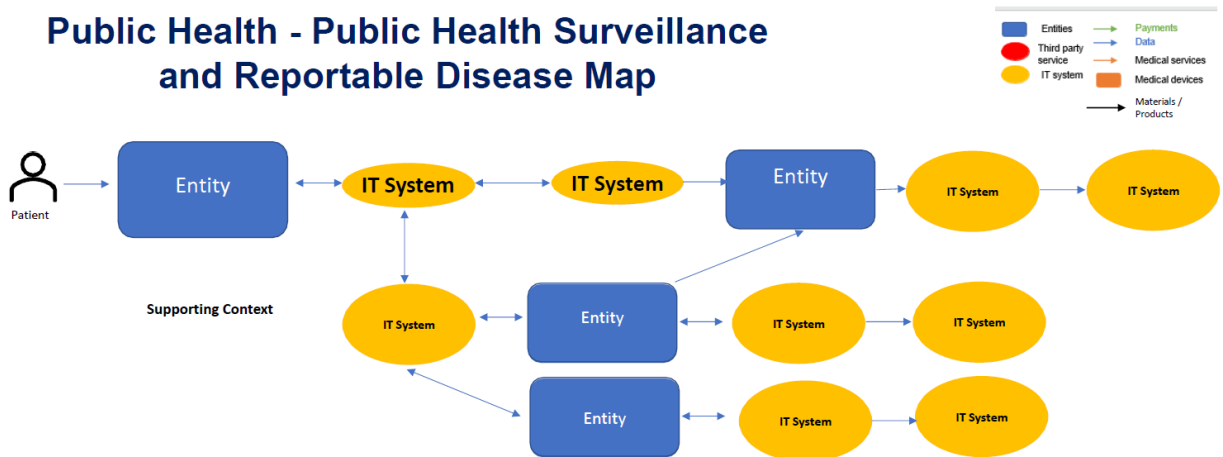
Map 11 Public Health Strategic National Stockpile

## Public Health – Strategic National Stockpile / Medical Counter Measure Distribution Storage and Administration



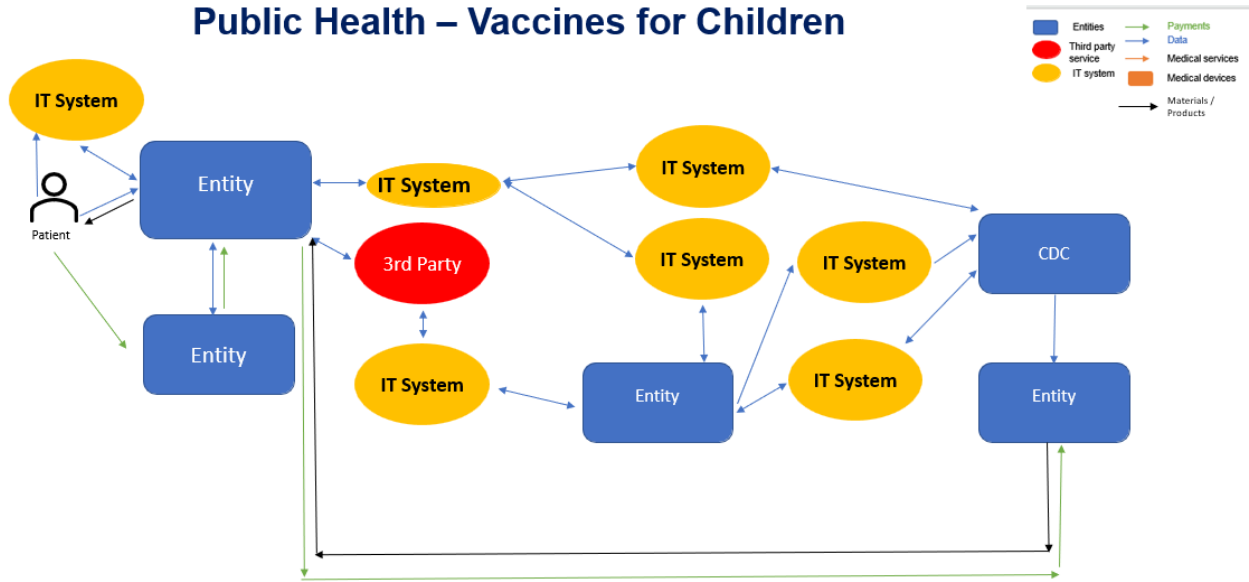
Map 12 Public Health Surveillance

## Public Health - Public Health Surveillance and Reportable Disease Map



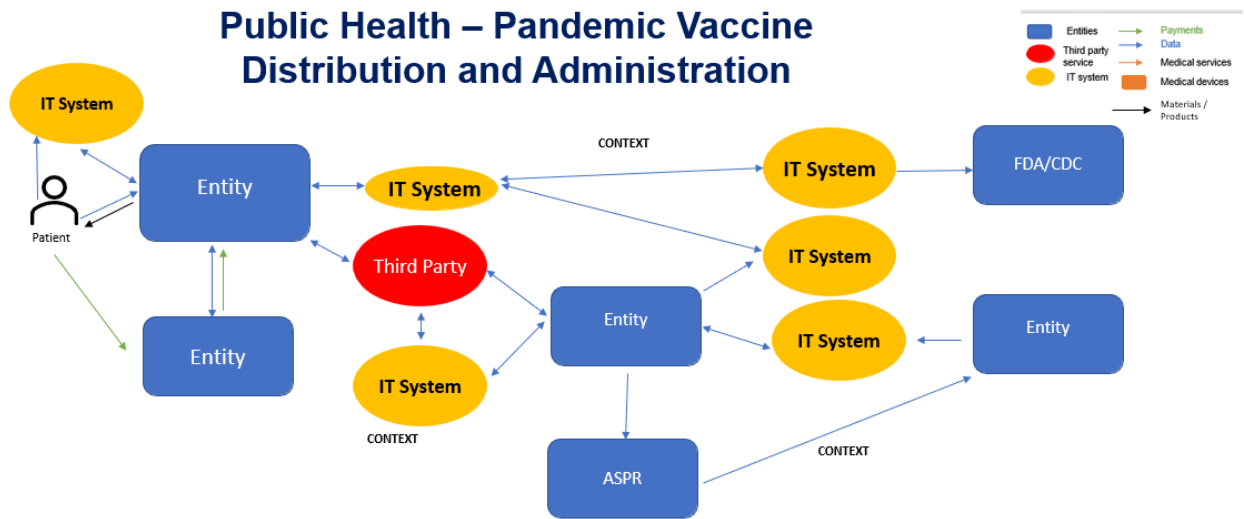
Map 13 Public Health Vaccines-Children

### Public Health – Vaccines for Children



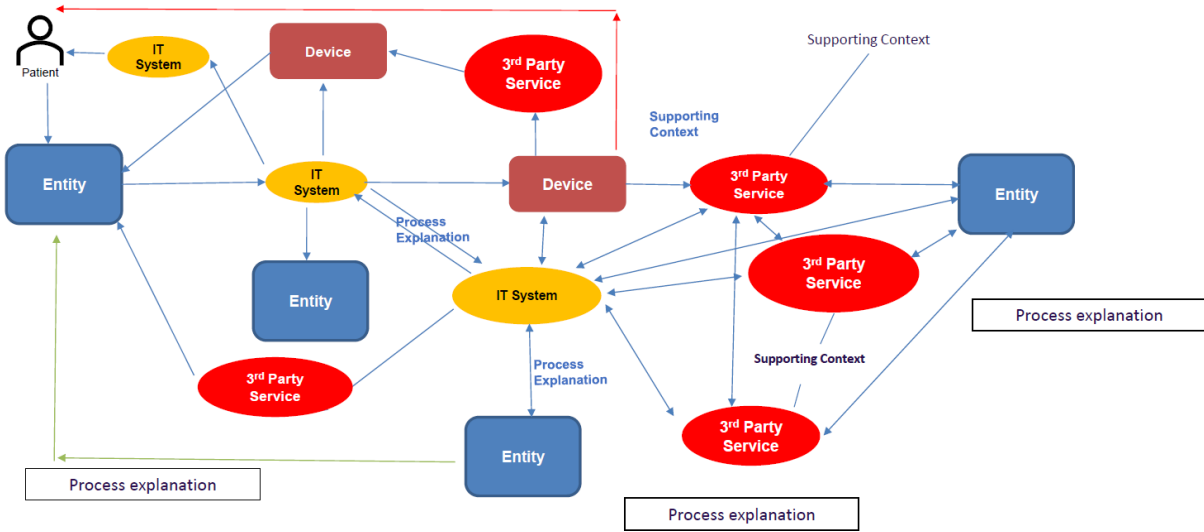
Map 14 Public Health Vaccines-Pandemic

### Public Health – Pandemic Vaccine Distribution and Administration



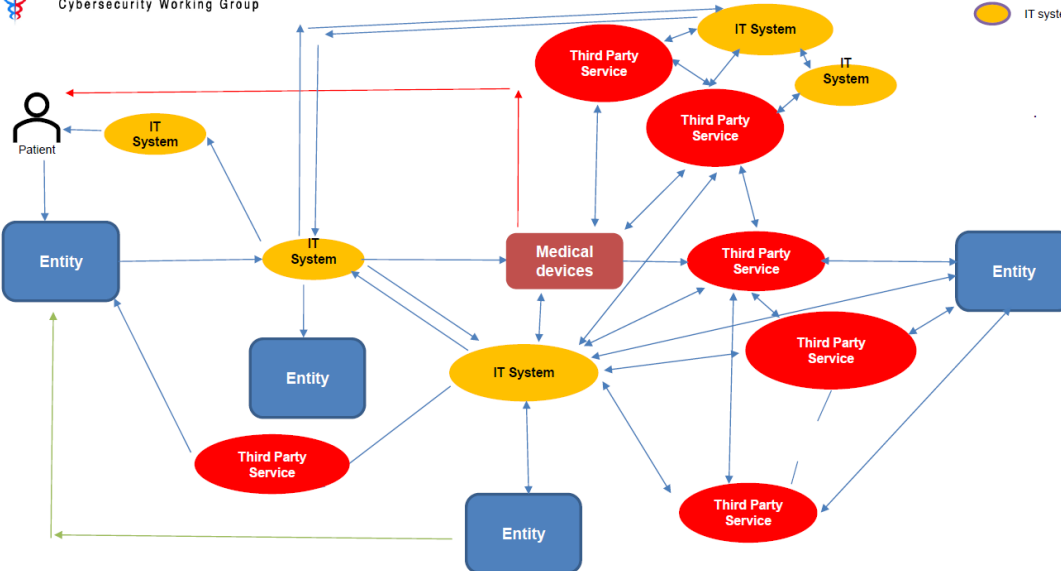
Map 15 Radiology-Diagnostic

### Diagnostic PACs/Radiology Systems



Map 16 Radiology-Therapeutic

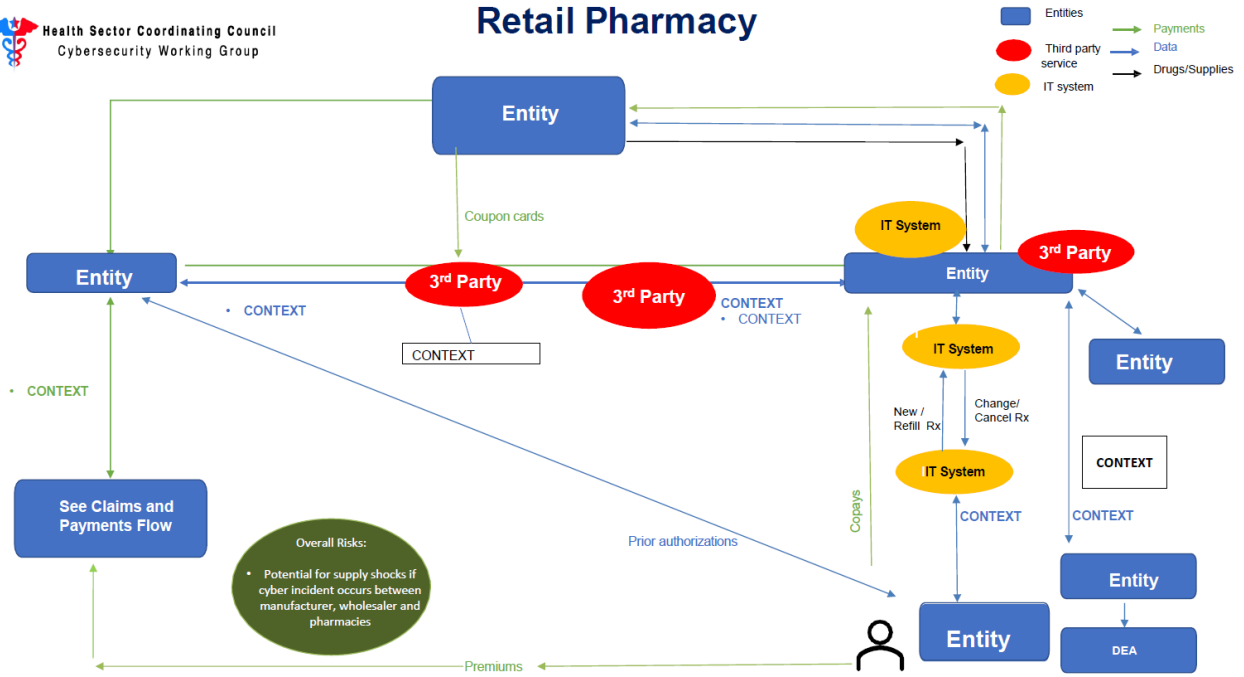
### Therapeutic PACs/Radiology Systems



# Map 17 Retail Pharmacy



## Retail Pharmacy



## Appendix B – Materiality

Organizations will vary on how they define materiality and who will define it, while ultimately owned by the board. This matrix shows how to measure and weight inherent risk exposure (impact x likelihood) through a rubric – tailored to enterprise – that considers impact to: Business, Finance, Safety, and Regulatory risk. The key is to get early agreement and alignment on materiality.

### Inherent Risk Exposure Rubric Example

Inherent Risk Exposure (Impact \* Likelihood) - Rubric

		Scale		1	2	3	4	5
Risk Impact How impactful / significant is the risk?	Impact		Low		Medium			High
	Description		A risk event would have <b>minimal</b> impact on business operations, finances, patient/caregiver safety, legal action, and organization overall.		A risk event would have <b>moderate</b> impact on business operations, finances, patient/caregiver safety, legal action, and organization overall.			A risk event would have <b>severe</b> impact on business operations, finances, patient/caregiver safety, legal action, and organization overall.
Attributes Level of impact	<b>Business Impact (BI)</b> - Strategic Impact (alignment with key objectives/initiatives) - Scope Impact (service area) - Reputation Impact (breadth of impact)	25%	<b>No significance or exposure</b> (Strategy - No discernable alignment Scope - Single Department Reputation - Internal (one facility))	<b>Minor significance and exposure</b> (Strategy - Relatively minor alignment Scope - Facility- or Clinic-Wide Reputation - Internal (multiple facilities))	<b>Moderate significance and exposure</b> (Strategy - Average alignment with potential challenges Scope - Regional Reputation - Regional)	<b>High significance with low to moderate exposure</b> (Strategy - Significant alignment with low impact Scope - Multiple Regions Reputation - Enterprise)	<b>High significance with high exposure</b> (Strategy - Significant alignment with high impact Scope - Enterprise Reputation - National)	
	<b>Financial (FIN)</b> - Financial Impact to Net Operating Income (NOI)	25%	< \$1 Million	\$1 - 25 Million	\$25 - 100 Million	\$100 - 250 Million	> \$250 Million	
	<b>Patient/Caregiver Safety (SAF)</b> - Unmitigated risk could result in...	25%	<b>No patient or caregiver harm</b>	<b>Near Miss</b>	<b>Preventable Event</b>	<b>Single Reportable Event</b>	<b>Multiple Reportable Events</b>	
	<b>Regulatory (REG)</b> - Impact of noncompliance with applicable laws and regulations - Frequency of changes to regulatory requirements	25%	<b>No Impact</b> (Impact - No impact to organization and/or subsidiaries Frequency - Informational updates only)	<b>Minor</b> (Impact - minimal Frequency - Limited or infrequent changes)	<b>Medium</b> (Impact - Narrow applicability (e.g., single program/service or location) Frequency - Minor revisions or occasional changes)	<b>Major</b> (Impact - Broad applicability (e.g., impacts multiple programs/services or locations) Frequency - New regulatory requirements or major/regular changes)	<b>Extensive</b> (Impact - Broad impact across enterprise or high dollar amounts Frequency - Extensive new regulatory requirements or significant/frequent changes)	
		Scale		1	2	3	4	5
Likelihood of Risk How likely is the risk?	Likelihood		Low		Medium			High
	Description		<b>Minimal</b> likelihood of risk being a threat to the organization.		<b>Moderate</b> likelihood of risk being a threat to the organization.			<b>High</b> likelihood of risk being a significant threat to the organization.
Attributes	<b>Probability (PROB)</b> - An estimation, before any risk response, that something will happen	50%	<b>Low</b> (Very low probability of risk event)	<b>Below Average</b> (Little probability of risk event)	<b>Average</b> (Occasional probability of risk event)	<b>Above Average</b> (Strong probability of risk event (Process not automated or performed by highly specialized individuals))		<b>High</b> (Very high probability of risk event)
	<b>Management's Confidence Level (MCL)</b> - Professional Judgement - Gut Check	50%	<b>Highly Confident</b> (Management believes there are strong internal controls and risk is consistently managed to the desired outcome)	<b>Confident</b> (Management believes the risk is typically managed to the desired outcome)	<b>Moderately Confident</b> (Management believes the risk is managed to the desired outcome at least half the time)	<b>Slightly Confident</b> (Management believes the risk is only occasionally managed to the desired outcome)		<b>Not Confident</b> (Management does not believe the risk is managed to the desired outcome and can provide specific examples)

# Control Environment Maturity Score Rubric

**1.**

Control Environment Maturity Score (Risk Mitigation) - Rubric							
Control Environment Maturity (Risk Mitigation)	Scale		5	4	3	2	1
	Maturity	Description	High		Medium		Low
Attributes	<b>Prior Assessments (PA)</b> - Include internal audits, external audits, consultants, and any other 'unbiased' evaluation of the department/process (including results of evaluation)	X%	<b>High</b> control environment maturity with strong risk mitigation activities in place. Environment regularly assessed.	<b>High</b> control environment maturity with strong risk mitigation activities in place. Environment regularly assessed.	<b>Medium</b> control environment maturity with average mitigation activities in place. Environment occasionally assessed.	<b>Medium</b> control environment maturity with average mitigation activities in place. Environment occasionally assessed.	<b>Low</b> control environment maturity with limited or no mitigation activities in place. Environment rarely assessed.
	<b>Oversight (OVER)</b> - Infrastructure - Accountability - Decision rights - Communication	X%	<b>Best Practice or Excellent</b> (- Infrastructure exists - Accountable Executive actively involved - Decision rights clear - Clear and timely communication)	<b>Good</b> (- Ad hoc infrastructure - Accountable Executive identified - Decision rights clear - Clear and timely communication)	<b>Average</b> (- Minimal infrastructure - Accountable Executive identified, but possible duplication of efforts - Decision rights unclear - Conflicting communications)	<b>Poor</b> (- Minimal infrastructure - Accountable Executive not identified or role confusion - Decision rights undetermined - Minimal communication)	<b>None or Very Poor</b> (- No evident infrastructure - No evident ownership - Decision rights undetermined - No communication)
	<b>Implementation (IMP)</b> - Standardization - Resources	X%	<b>Best Practice or Excellent</b> (- Standardization embraced - Resources adequate for process implementation)	<b>Good</b> (- Standardization understood, generally accepted and implemented - Resources available, shuffled as needed)	<b>Average</b> (- Process customized/varied locally - Resources temporarily allocated)	<b>Poor</b> (- Process variation/ambiguity - Identified inadequacy of resources)	<b>None or Very Poor</b> (- No accepted process - No resources identified or defined)
	<b>Policies, Procedures, Guidelines (PPGs) &amp; Education</b> - Establishment of PPGs - Education of workforce	X%	<b>Best Practice or Excellent</b> (- All PPGs known - All required PPGs exist - All PPGs reviewed on schedule - Clarity of audience & standard content/delivery - Education completion is tracked)	<b>Good</b> (- Most PPGs known - Most required PPGs exist - All PPGs reviewed in last 3 years - Clarity of audience & standard content/delivery - Education completion is not tracked)	<b>Average</b> (- Some PPGs known - Some required PPGs exist - Some PPGs are overdue for review - Audience is undefined & content is not standard or ad hoc delivery - Education completion is not tracked)	<b>Poor</b> (- Unknown what PPGs are needed - Unknown if required PPGs exist - Most PPGs are overdue for review - Education does not exist)	<b>None or Very Poor</b> (- PPGs do not exist - PPGs exist, but are all overdue for review - Education requirements have not been identified)
	<b>Monitoring (MON)</b> - Metric maturity - Monitoring activities and frequency	X%	<b>Best Practice or Excellent</b> (- Optimized metrics - Automated process monitors - Issues consistently reviewed)	<b>Good</b> (- Managed metrics - Monitoring performed consistently; manual/resource intensive - Issue not consistently reviewed)	<b>Average</b> (- Defined metrics - Process monitors sporadic - Reviews based on sentinel events)	<b>Poor</b> (- Repeatable metrics - Process monitors not standardized - Variation between facilities)	<b>None or Very Poor</b> (- Initial or no metrics - No process monitoring)

## Example Template

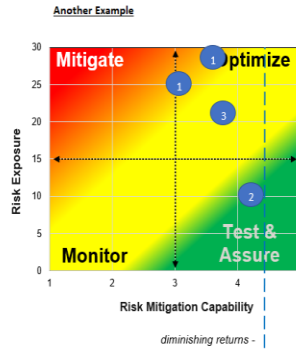
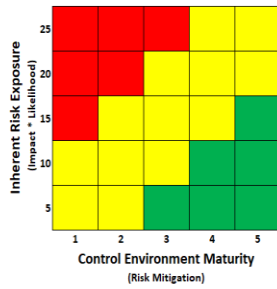
Risks & Inherent Risk Exposure			Risk Impact (I)					Probability of Risk (P)			FY2023 Risk Exposure (I*P)		FY2024 Risk Exposure (I*P)	
ID	Risk	Description	25% BI	25% FIN	25% SAF	25% REG	50% PROB	50% MCL	50%	50%				
			Business Impact	Financial	Patient/Caregiver Safety	Regulatory	Probability	Management's Confidence Level						
A			5 Notes/Rationale	5	4	5	5	5	5	5			29.8	
B			5 Notes/Rationale	5 Notes/Rationale	5	4	5	5	2	2			16.6	
C			5	4	5	3	3	3	2	2			10.6	
D			3	3	3	3	3	3	2	2			7.5	
E			1	1	1	2	2	2	1	1			1.9	

Control Environment Maturity (Risk Mitigation)			Control Environment Maturity (Risk Mitigation)					Risk Affinity Team Sponsor?		FY2023 Risk Mitigation Score		FY2024 Risk Mitigation Score	
ID	Risk	Control Measures/Risk Mitigation Activities	20% PA	20% OVER	20% IMP	20% PPG	20% MON						
			Prior Assessments	Oversight	Implementation	Policies, Procedures, Guidelines & Education	Monitoring						
A			1 Notes/Rationale	1	1	1	1						1.0
B			3	2	3	2	1						2.2
C			4	2	3	3	2						2.8
D			5	5	5	3	3						4.2
E			5	5	5	5	5						5.0

# Heat Map Example

## Heat MAP Example



**Risk Response Strategy**

- Mitigate**
  - > Risk mitigation capabilities need to be added.
  - > Primary focus area for internal audit activities.
- Monitor & Optimize**
  - > Enhance and monitor existing capabilities as appropriate. Additional resources or investment may be necessary.
  - > Primarily managed by 2<sup>nd</sup> line of defense functions (e.g., Compliance, Quality & Safety, Risk Management)
- Test & Assure**
  - > Strong mitigation capabilities are in place.
  - > Business and front-line staff own their respective risk mitigation activities.

## Keys to Scoring / Guiding Principles

### Be Consistent

Give the same scores for the same quality & quantity of information for each risk area.

### Use your professional judgment

As you look through your scoring if something doesn't feel right, pass the smell test, etc., then re-examine that area.

### Balance thoroughness with common sense

It's okay for some areas to be "average area of risk" and limited comment. Some areas aren't that tricky.

### Know your limits

You are not an expert at everything and you cannot know everything. If you need more understanding of an area ASK!

### Regional vs Enterprise

Balance Regional control environment maturity with One Intermountain (enterprise) maturity. Where have processes been centralized? Are there regional specific risks?

## Appendix C: Excel Template for Supplier and Services Critical Function Analysis

<b>Critical Function:</b>	
<b>Vendor:</b>	
<b>Service/Product:</b>	
<b>Operational Impact:</b>	
Critical Function Impacts:	
Process Impacts:	
Short Term Consequences:	
Long Term Consequences:	
<b>Identify Mitigations in Place:</b>	
Existing Work Arounds?	
Effectiveness of Mitigations?	
<b>Scope of Material Impact:</b>	
Impact Size (isolated vs system wide)	
Financial Impact:	
<b>Chokepoints/Risk Concentrations:</b>	
Identify Chokepoints:	
Identify Risk Concentrations:	
<b>Is this vendor a priority for further risk mitigations?</b>	

---

## Appendix D – Systemic Risk Governance Policy Template (including RACI diagram)

# [Organization] Systemic Risk Governance Policy

Version: [Year/no]

Document status: Draft or Final

Date issued: [date]

Approved by: [insert organization name]’s Risk Committee of Board of Directors on [date]

Date for review: [date]

### Record of policy development:

Version number	Date of issue	Lead author/reviewer	Consultative panel	Significant changes on previous version
[Yr/no]	[Date]	[Name/role]	[Name/role/organization]	[For example, incorporate changes to new legislation]

### #Note\*

*This policy template has been developed to meet the needs of a diverse range of services and includes items for consideration in policy and procedure.*

***Not all content will be relevant to your organization. Organizations are encouraged to edit, add and delete content to ensure relevancy.***

*All notes (like this one) should be considered and deleted before finalizing the policy, and the contents list should be updated as changes are made and when content is finalized.*

*\*Please delete note before finalizing this policy.*

## SECTION 1: SYSTEMIC RISK COMMITTEE GOVERNANCE POLICY FRAMEWORK

### 1.1 Policy statement

[Insert organization name]’s Systemic Risk Committee is governed by the Risk Committee of the Board of Directors acting on behalf of [insert organization name]. The Board is committed to providing effective oversight of the organization, setting the strategic direction, managing risk, and ensuring organizational viability.

### 1.2 Purpose and scope

The purpose of this Systemic Risk Committee Governance Policy is to provide guidance to the committee in their role of identification of systemic risks and process to remediate those risks to a level acceptable to the organization.

Systemic risks are defined as ones that would cause irreparable harm to the organization, making it non-viable. These risks may cause impacts that affect patients/staff, revenue, or have legal ramifications to the organization.

### 1.3 Definitions

<b>Board/Board of Directors</b>	The legally responsible managing body of the organization.
<b>Risk Committee</b>	Subcommittee of the Board of Directors to which the Systemic Risk Committee Reports.
<b>Governance</b>	Rules and structures setting out how an committee is managed.
Add additional as needed	

### 1.4 Principles

1. **[Insert organization name]**'s views good governance and management practice as essential to fulfilling its goal in a responsible manner.
2. The Board conducts its affairs legally, ethically and with transparency.
3. The Systemic Risk Committee will ensure that risks from across the organization are identified and ranked, and that appropriate risk mitigation/remediation plans are put in place.

### 1.5 Outcomes

1. **[Insert organization name]**'s governance practice contributes to a quality organization that meets its mission and vision.
2. Systemic organizational risks are identified and managed/mitigated through policies, procedures and practice improvement.
  - a. Systemic risks are identified regularly.
  - b. Remediation plans to mitigate those risks are identified, implemented, and monitored.

### 1.6 Committee Members and Roles and Responsibilities

The RACI diagram below shows the typical members of the systemic risk committee and their roles and responsibilities. Members should be added or removed based on the needs of the organization. The membership of the committee must have a good mix of experienced and knowledgeable people and allows for discussion and identification of existing processes to a highly specific level that allows identification of systemic risk. Additionally, members should have the authority to implement approved remediations against identified risk and monitor their effectiveness on a continual basis. These roles and responsibilities generally require individuals in leadership positions; however, in some workflows and areas subject matter experts without lower-level decisional or management authority may be required to provide information to ensure the understanding of the workflow or ecosystem.

## RACI diagram

R = Responsible

A = Accountable

I = Informed

C = Consulted

Team Member/ Responsibility	Lead Committee	Facilitate Identification of Risk	Identify Mitigations for Risk	Implement Mitigations for Risk	Monitor Mitigations	Report to Board
Risk Management Leader	A	R	I	I	I	A
Legal Leader		R	R	R/I	I	
Compliance Leader		R	R	R/I	I	R
Information Technology Leader(s)		R	R	R/I	R/I	R
Cybersecurity Risk Management (GRC) Leader	R	A	R	R/I	R/I	R
Other Support Area Leaders (e.g Security, Facilities, Clinical Engineering, etc).		R	R/I	R/I	R/I/C	R
Operational Leaders/ Workflow Subject Matter Expert		R	R/I	R/I	R	R
Finance Leader		R	R/I	R/I	R/I/C	R
Supply Chain Leader		R	R/I	R/I	R	R
Other Leaders as needed		R	R/I	R/I	R	R

### 1.7 Risk management

This Policy and its procedures are informed by and comply with **[insert organization name]**'s regulations.

This Governance Policy is included in **[insert organization name]**'s policy review schedule where all policies are reviewed every **[Insert frequency]** at a minimum, or following significant operational, policy or legislative requirements.

The critical function maps used to help identify systemic risk developed by the Health Sector Coordinating Council provide information that identify general workflows. These maps contain information that may be useful to threat actors and other parties looking to disrupt organizations' business for varied purposes including ransom, and therefore the maps will be held in strictest confidence by the committee and not shared outside the organization. For more information on the confidentiality of these maps, please see the Health Sector Coordinating Council website at <https://HealthSectorCouncil.Org/workflow-maps-request>.

## **SECTION 2: Procedures**

### 2.1 Risk Identification

The Systemic Risk Committee will follow the risk management identification process outlined in this Health Sector Coordinating Council document “Sector Mapping and Risk Toolkit”. This process should be completed initially to identify systemic risk within the organization and repeated as circumstances evolve within the organization. Upon completion of the Risk Identification phase, the committee will determine how often the systemic risks and workflows should be reviewed so that ongoing and new risks will continue to be identified on a continual basis.

### 2.2. Risk Mitigation

As Systemic Risks are identified, the Systemic Risk Committee will create options for various mechanisms or mitigations to reduce or eliminate the risk identified. The Committee will assign those mitigations to the appropriate party for implementation and monitor the implementation. Measurement of the residual risk should continue to be tracked and reported to the Risk Subcommittee of the Board.

Risk Mitigation plans should be re-evaluated on an annual basis to ensure that they continue to meet the needs of the organization.

## **SECTION 3: BOARD AND SYSTEMIC RISK COMMITTEE RELATIONSHIP**

### 3.1 Relationship between the Board and Committee

On no less than an annual basis, the committee will present a summary of identified systemic risks to the Risk Subcommittee of the Board of Directors.

The identified risks will be ranked against overall risk to the organization and reports will summarize the effectiveness of implemented mitigations. The Risk Subcommittee will continue to monitor risk mitigations to ensure that identified systemic risks are appropriately reduced.

---

## **Appendix E: Example Scenario**

To help organizations understand and apply this process, a fictitious scenario will illustrate this process using one element of the critical function maps. This example is for guidance purposes only.

**Scenario:** A medium-sized hospital with inpatient and outpatient services has decided to identify and prioritize its third-party risk related to its supply chain using the process set out in the SMART document. The CISO is concerned about recent events related to breaches with industry wide impacts and wants to begin identifying other major third parties that would impact hospital operations.

## Phase 1: Risk Identification Process

### Step 1: Build Collaborative Team

The Hospital's CISO forms a collaborative team that includes the following:

- Director of Compliance/Risk
- CFO/Director of Finance
- CIO/Director of IT
- Chief Nursing Officer
- Director of Supply Chain
- Marketing/Communications
- Legal

### Step 2: Define Materiality

The team agrees to a definition of what is “material” in their organization. This generally follows the Inherent Risk Rubric in [Appendix B](#).

The team determined that on-hand supplies in the system are limited to approximately 2 business days and any disruption that affects the supply chain longer than this will require some intervention to keep the hospital functioning.

Service lines are prioritized based on the revenue they bring to the hospital (Business Risk). Guidelines are developed for when the emergency department and other critical care areas would be functional and at what point the hospital would have to go on diversion (Patient Safety).

Discussions identify the current controls in place to mitigate possible scenarios. The team decides the business impact is high as the loss of a supplier's ability to deliver its requirements would cause units to close based on the priority discussed. Lost patient volume would correspondingly reduce hospital revenue. The event would likely cause multiple patient safety events and a major regulatory impact. The probability of the event occurring is variable depending on the type of event. The team discussed several scenarios including:

- Long term disruptions such as losing the primary supply distributor due to a cyber event
- Medium term mass disruptions as a result of bad weather or strikes affecting national delivery vendors
- Short term small disruptions due to recalls or back-order situations

The team determined that the overall probability of the event based on the above was moderate. The team then discussed what mitigations are currently in place, and which are not robust.

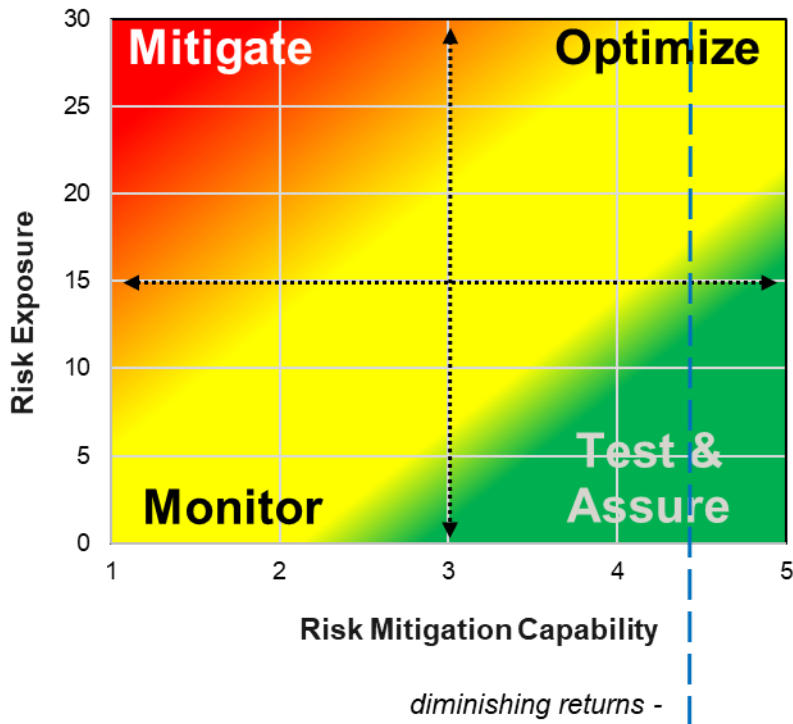
The following Risk & Inherent Risk Exposure document was created using the template to document those decisions. The overall risk exposure score is calculated by taking a weighted average of the risk impact score and multiplying it by a weighted average of the probability of risk.

Risks and Inherent Risk Exposure			Risk Impact (RI)								Probability of Risk (PI)				Risk Exposure (RI*IP)
			BI		FIN		SAP		REG		PROB		MGL		
ID	Risk	Description	25%	Business Impact	25%	Financial	25%	Patient / Caregiver Safety	25%	Regulatory	50%	Probability	50%	Management's Confidence Level	
A	Supply Chain Risk	Lose Ability to order, obtain and deliver supplies to run the facility.	5	Shut units, Divert Patients	5	Lost Revenue form Diversion	5	Multiple events	4	Major	4	Moderate	5	Not Confident	21.375
B															
C															
D															

The team then discussed the control environment maturity or risk mitigations currently in place, again using the template in [Appendix B](#). There was no prior assessment performed for this risk. The oversight for this area is deemed average and the implementation poor. The policies, procedures, guidelines and education are deemed average as is the monitoring. These scores are then averaged together to get the Risk Mitigation Score.

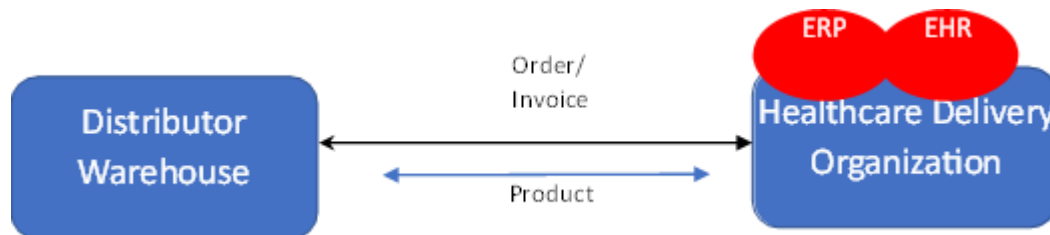
Control Environment Maturity (Risk Mitigation)			Control Environment Maturity (Risk Mitigation)											Risk Mitigation Calculation	
			PA		OVER		IMP		PPG		MON		Response Risk Strategy		
ID	Risk	Control Measures / Risk Mitigation Activities	20%	Prior Assessments	20%	Over-sight	20%	Implemen-tation	20%	Policies, Procedures Guidelines, and Education	20%	Monitor-ing			
A	Supply Chain Risk	Lose Ability to order, obtain and deliver supplies to run the facility.	1	No Assessments	3	Average	2	Poor	3	Average	3	Average		Mitigate	2.4
B															

The heatmap then is used to plot the risk exposure score on the Y-Axis and the Risk Mitigation Capability on the X-Axis. The quadrant plots the result and the Response Risk Strategy to implement. In this case, the strategy is to Mitigate the risk.



### Step 3: Review all Critical Function Maps

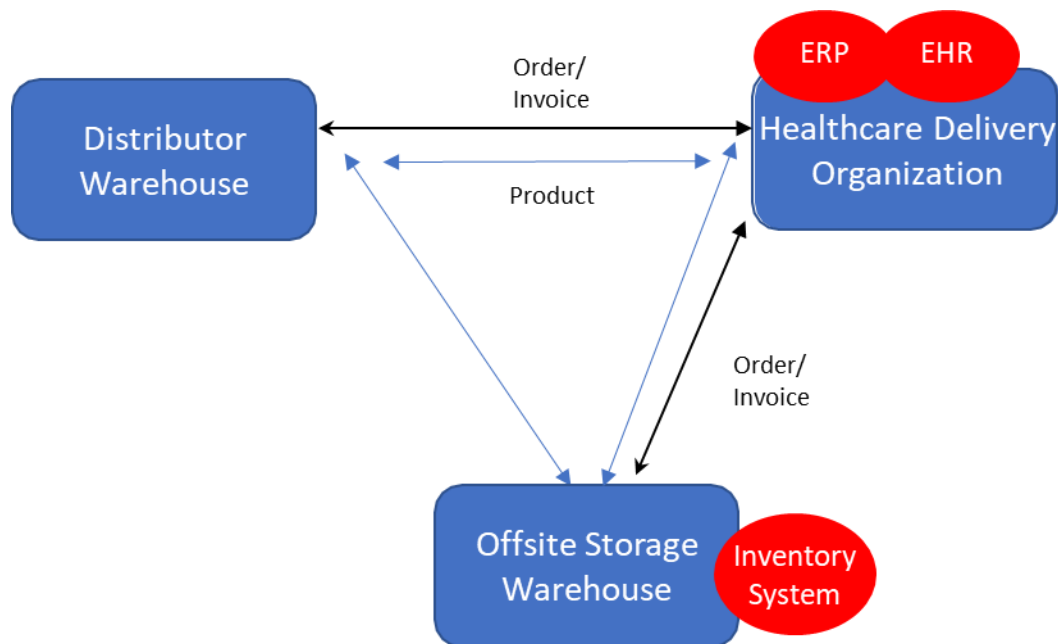
The cross functional team reviewed all Critical Maps and chose which maps to focus on. The team chose the three Supply Chain Maps - Pharmaceuticals, Medical Products, and Medical Devices. Note: for this example, focus only on this portion of the Medical Products and Distribution Map which highlight the relationship between the hospital and their distributor. This reduction in size/scope is only to keep the example a reasonable length.



#### Step 4: Customize the Prioritized Map

The team then discusses how the provided maps need to be adapted to the different workflows that occur at the hospital.

- 1) There is an electronic system that exchanges the Order/Invoice between the Distributor and the healthcare delivery organization. That system interfaces with the ERP to generate the order and accept the invoice.
- 2) The EHR interfaces with the ERP to provide details about cases that will require specialty supplies like tissues and implants.
- 3) The products shipped from the distributor can take alternate paths:
  - a) Directly to the healthcare delivery organization via normal delivery
  - b) Directly to the healthcare delivery organization via expedited shipping
  - c) Shipped to the organization's third-party warehouse for storage.
- 4) The third-party warehouse also has its own inventory management system which is integrated with the hospital's ERP system. Orders and Invoices transmit through this integration.
- 5) Products from the third-party warehouse can also be delivered to the healthcare delivery system via normal delivery, or via expedited shipping
- 6) There is also a process for products to be returned to the distributor or stored in the offsite storage location. These are communicated through the inventory system/ERP interfaces.



## Step 5: Identify Vendors and their Services/Products

For this example, we will keep generic vendor names.

- Distributor Ordering System
- HDO ERP
- HDO EHR
- HDO Order Transmittal System
- HDO Interface Engine (that drives the system interfaces for all systems)
- Offsite Storage Inventory Warehouse System
- Delivery Vendor Tracking System
- Expedited Delivery Vendor Tracking System

## Step 6: Conduct Critical Function Analysis

For this example, we assess two of the above identified vendors using the template in [Appendix C](#):

Critical Function	Supply Distribution
Vendor	Distributor
Service/Product	Ordering System
Operational Impact	
<b>Critical Function Impacts</b>	If the distributor's ordering system is not available, no supplies can be ordered. In the immediate term, phone calls to the vendor would be made to see if phone orders or some other verbal/fax process could be accepted. If no orders can be placed, there is immediate risk to the organization as there usually are only 2 days of stock on hand.
<b>Process Impacts</b>	Pull available stock in offsite storage. Immediately inventory current stock in hospital. Assess patient population, elective and critical cases and determine what cases can and cannot continue. Identify alternate vendors for all products (there are thousands of line items). Identify high risk products that require additional staff training. Order critical supplies at possibly higher cost.
<b>Short Term Consequences</b>	Delayed delivery of supplies from new vendors, rationing of supplies, possible cancellation of elective surgery, negotiation with other distributors for supplies (at possibly a higher cost). Patient risk increases due to staff's inadequate product knowledge.
<b>Long Term Consequences</b>	Competition from other hospitals for the same supplies (don't assume our organization is the only one affected), supply shortages and backorders, constant substitutions, patient risk due to staff's inadequate product knowledge. Higher costs from possibly additional supply chain staff to find, order, and manage the multiple replacement

	vendors/rolling backorders. Higher supply costs overall. Possible reputational damage and legal impact.
<b>Identify Mitigations in Place</b>	
<b>Existing Work Arouds</b>	About 1/8 of supply list has identified substitutions.
<b>Effectiveness of Mitigations</b>	Minimal
<b>Scope of Material Impact</b>	
<b>Impact Size (isolated vs Organization wide)</b>	Organization Wide
<b>Financial Impact</b>	Significant
<b>Chokepoints/Risk Concentrations</b>	
<b>Identify Chokepoints</b>	All orders go through one distributor via one ordering process.
<b>Identify Risk Concentrations</b>	Currently have only one primary distribution agreement. No backup agreement exists.
<b>Is this vendor a priority for further risk mitigations?</b>	Yes
<b>Critical Function</b>	
	Supply Distribution
<b>Vendor</b>	Offsite Inventory Warehouse
<b>Service/Product</b>	Inventory System
<b>Operational Impact</b>	
<b>Critical Function Impacts</b>	If the offsite warehouse loses the use of its inventory system, the organization would not be able to order/pull items out of storage and not be able to send items to storage.
<b>Process Impacts</b>	Excess supplies and supplies held here would not be accessible. Would need to transition to a just-in-time delivery from the distributor causing disruption to normal processes.
<b>Short Term Consequences</b>	Several major departments that routinely use the offsite inventory warehouse would have to change their workflows to move to a just-in-time ordering/utilization model. This would impact patient flow moderately for a short time and require some additional staff during the disruption.
<b>Long Term Consequences</b>	Same as short term consequences.
<b>Identify Mitigations in Place</b>	

<b>Existing Work Arounds</b>	Utilize just in time ordering and delivery. Use additional staff (temporary) to minimize patient flow and departmental process impacts. Additional overnight shipping may be required.
<b>Effectiveness of Mitigations</b>	Effective
<b>Scope of Material Impact</b>	
<b>Impact Size (isolated vs Organization wide)</b>	Isolated to a few departments
<b>Financial Impact</b>	Minimal to the organization, moderate to the affected departments
<b>Chokepoints/Risk Concentrations</b>	
<b>Identify Chokepoints</b>	Single system used by offsite storage warehouse for inventory management, invoicing, and billing.
<b>Identify Risk Concentrations</b>	The organization has only one outside warehouse location identified.
<b>Is this vendor a priority for further risk mitigation?</b>	No.

Phase 2: Mitigations and Action Plans

Once all vendors have been assessed, the vendors that were identified as requiring further risk mitigations move onto phase 2.

These mitigation plans should include reviewing the initial vendor questionnaire (if it was completed) when the vendor was on-boarded. The CISO team should conduct an initial vendor assessment if not already done. This may include regulatory requirements or best practices including SBOMS, contingency plans, patch management plans and secure-by-design principles.

Any areas identified in the vendor assessment should be catalogued and discussed with the vendor, and mitigation plans should be built, monitored, and reported on regularly. Ongoing communication with the vendor is critical to ensure timely resolution of all identified risks.

Additionally, contract language may stipulate requirements such as reporting timelines for breaches, ability to audit, etc. that are identified as critical to the organization. Vendor compliance with these added contractual obligations should be monitored on a regular schedule for needed remediation depending on the materiality of the vendor.

In addition, operational plans (disaster recovery or downtime plans) should be built by the business owner to further strengthen the resiliency of the organization. Tabletop exercises can also be used to train staff and practice plans so they can be refined for the preparedness of the organization.

In this particular example, operational plans may include onboarding a secondary supply vendor and cross-walking all critical supplies so that immediate failover can activate in the event of a downtime situation.

---

## Glossary

This section attempts to overcome challenging terminology discrepancies unique to the health sector. Not all these terms are found in this document but are found in the critical function maps. Several maps use these acronyms to aid in visualization of flows. Additionally, hyperlinks are available for those terms that relate to government agencies that point to their official webpages.

**[ASPR](#)**: Administration for Strategic Preparedness and Response. An agency under the Department of Health and Human Services that leads the nation's medical and public preparedness for, response to, and recovery from disasters and public health emergencies.

**[CDC](#)**: Centers for Disease Control. The nation's leading science-based, data-driven, service organization that protects the public's health.

**[CMS](#)**: Centers for Medicare and Medicaid Services. The federal agency that provides health coverage to more than 160 million through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace. CMS is part of the Department of Health and Human Services (HHS).

**Critical functions**: Functions within the health sector that must continue to operate for patient care, liquidity, and operational continuity. They are generally interconnected and interdependent on the availability and integrity of various IT and 3<sup>rd</sup> party systems and services to operate. Other risks (such as, but not limited to, utilities, market consolidation, and geopolitics) may also influence the performance of these functions.

**CRM**: Customer Relations Management software. This is software businesses use to interact with their customers and can help with sales, marketing efforts, and customer support.

**[DEA](#)**: Drug Enforcement Administration. United States federal law enforcement agency that is under the Department of Justice (DOJ).

**DICOM**: Digital Imaging and Communication in Medicine. A standard that specifies a non-proprietary data interchange protocol, digital image format, and file structure for biomedical images and image related information.

**EDI**: Electronic Data Interchange. A secure automated exchange of data and documents between organizations or entities that allows for different computer systems to communicate with each other.

**EHR**: Electronic Health Record. A digital record of a patient's medical history that can be shared across multiple health providers. This is often confused with an **EMR** (Electronic Medical Record). Electronic medical records are digital versions of paper charts that are local to a single provider and are not shared by the provider.

**Entity (Entities)**: A single organization or entity that performs a critical function identified in a workflow map. These entities can be physical or virtual and are interconnected and interdependent. They are held responsible for response and recovery after an event.

**ERP:** Enterprise Resource Planning system. This system is generally a software-based platform that helps organizations manage and automate core business processes such as supply chain, inventory management, and finance.

**FDA:** Food and Drug Administration. United States Government Agency under the Department of Health and Human Services (HHS) that regulates the safety of food, drugs, and medical devices.

**Healthcare Delivery Organization:** Any organization that provides clinical and medical services to patients including, but not limited to, healthcare systems, hospitals, clinics, private physicians' office, skilled nursing facilities, long term care facilities, nursing homes, and home health agencies. These organizations can be private (for profit or non-for profit) entities, entities run by the US government (e.g. VHA, DOD, DNS, NIH, etc), or Tribal organizations. They may also include organizations such as retail pharmacies that provide services such as vaccinations to the public and even some insurers who provide resources such as durable medical equipment or pharmaceuticals directly to patients.

**HHS:** Health and Human Services. A cabinet level executive branch department of the United States Federal Government with a mission to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.

**HIE:** Health Information Exchange. Electronic system that allows patients and healthcare providers to share patient's medical information.

**IZ Gateway:** Immunization Gateway. Interjurisdictional Public Health IT infrastructure which supports the exchange of immunization data between immunization information systems (IISs). The IZ Gateway is a program that includes a technology solution and infrastructure that facilitate immunization data exchange. It securely supports efficient exchange of immunization data among jurisdictional immunization information systems (IIS) and between IISs and public and private vaccine-providing organizations (e.g., Veterans Health Administration, physician's offices, pharmacies).

**LIS:** Laboratory Information System. Computer system used in medical settings to manage and store all aspects of patient laboratory data and workflow including orders, results, and patient information.

**Medical Device:** Product regulated by Food and Drug Administration (FDA); for example, a tool, machine or other instrument or software used to diagnose, treat or prevent disease or other condition.

**NNDSS:** The National Notifiable Disease Surveillance System. A nationwide collaboration that enables all levels of public health (state, local, tribal, territorial, federal, and international) to share health information to monitor, control, and prevent the occurrence and spread of state-reportable and nationally notifiable infectious and some noninfectious diseases and conditions.

**PACS:** Picture Archiving and Communication System: Medical imaging technology used in organizations to securely store and digitally transmit electronic images from various modalities and clinically relevant reports.

**PBM:** Pharmacy Benefit Manager. A third-party company that manages prescription drug programs for various clients, including but not limited to: Health insurers, Medicare Part D plans, large employers, federal and state programs, and self-insured employer plans.

**PCI DSS:** Payment Card Industry Data Security Standard. National standard issued by the Payment Card Security Standards Council which applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. These standards are followed in order to allow all organizations the ability to accept credit and debit card transactions.

**QMS** – Quality Management System. A system that defines and documents an organization's business processes, procedures, and responsibilities for achieving quality policies, practices, and objectives to achieve compliance with regulations. QMS regulations are governed by either ISO 13485 or Good Manufacturing Practice FDA regulations 21 CFR 820.

**RIS** – Radiology Information System. Computer system that manages patient information, patient scheduling, medical imaging and associated data for radiology departments.

**Vendor:** Third-party that provides services or product to a hospital or health provider

**VNA:** Vendor Neutral Archive. Software application that stores medical images in a standard format regardless of vendor.

**VTrcks:** Vaccine Tracking System. A vaccine management application that allows CDC and healthcare providers to order and manage publicly funded vaccines.

---

## Acknowledgments

The SMART Co-Leads are grateful for the significant investment of personal time by all the authors of this document in its creation. The authors represent some of the most skilled and experienced experts in their field and this document would not have been possible without their generosity, leadership and commitment to a more secure health sector. Significant contributors are identified with an asterisk by their name. We would also like to acknowledge the support of the authors' employers in lending their employees' time, office facilities and information technology infrastructure in the development of this material. We are grateful for the leadership and editorial skills of Greg Garcia, Executive Director of the HSCC-CWG and the operational support of Allison Burke.

While many individuals assisted in the development and review of this content, the primary authors across this document and version were:

### Co-Leads

Samantha Jacques*	McLaren Health
Adrian Mayers*	Premera BlueCross
Charlee Hess*	HHS Administration for Strategic Preparedness and Response

### Contributors

Oluwashina Joseph Ajayi	Baxter Healthcare
Edison Alvarez	Becton Dickinson and Co
Alexander Arango	Nomi Health
Janette Arencibia	Defense Health Agency
Raj Atluri	North Kansas City Hospital and Meritas Health
Jeff Bontsas	Ascension
Robert Bastani*	HHS Administration for Strategic Preparedness and Response
Debra Bruemmer*	MedSec
Maria Cante	Defense Health Agency
Matt Christensen*	Intermountain Health
James Coburn	U.S. Food and Drug Administration
Bridnusa Curcaneanu*	NeuroPace
Philip Curran	Cooper University Healthcare
Cari Daniels*	UNC Health
Erik Decker*	Intermountain Health
Jack Dimpsey III	Oklahoma State Department of Health
Mark Early	Adena Health System
Phil Englert*	Health Information Sharing and Analysis Center (Health-ISAC)
Sahan Fernando	Rady Children's Hospital
Ed Gaudet*	Censinet
Scott Gee*	American Hospital Association

Erin Gilliam	Merck
Chris Graham	Presbyterian Healthcare Services
Ty Greenlaugh*	Medigate by Claroty
Mark Green	Availity
Andrea Green-Horace*	HHS Centers for Medicare & Medicaid Services
Garrett Hagood*	Coastal Bend Regional Advisory Council
Matthew Halvorsen*	Exiger
Jacob Hammersmith	Billings Clinic
Judy Hatchett*	Surescripts
Rick Hampton*	Rick Hampton Advisors
Dan Holland	Tampa General Health System
Tom Horton	Weill Cornell Medicine
Lexi Humphreys	Veradigm
Shawn Keeley	BlueCross BlueShield of Rhode Island
Ishan Khadka	Cape Cod Healthcare
Puja Khare	Greater New York Hospital Association
Sydney Klein	Bristol Myers Squibb
Shannon Lantzy*	Shannon Lantzy LLC
Christopher Lugo	BlueCross BlueShield Association
Robert Maclay	Stanford Medicine Children's Health
Geoffery Mann*	Health Information Sharing and Analysis Center (Health-ISAC)
Janine Medina	Thermo Fisher Scientific
Caleb Merriman	Highmark Health
Delara Mohtasham	Baxter Healthcare Corporation
David Nathans	Siemens Healthineers
Leslie O'Connor*	Labcorp
Charity Otwell	Center for Internet Security
Andy Price	St. Clair HealthCare
Mike Ratliff	Providence
Bill Reid*	Google
Jim Roeder	Lakewood Health System
Terri Rice*	Merck Inc.
John Riggi*	American Hospital Association
Kennyon Sadler*	Veterans Affairs
Sanjeev Sah	Novant Healthcare
Blake Scott*	Coconino County Health and Human Services
Mosa Shahzada*	Exiger
Philip Shen	Memorial Sloan Kettering Cancer Center
Dallas Smith	Burn and Reconstruction Centers of America
Mark Snyder	Intuitive Surgical

Matt Solomon	Humana Inc
Anthony Soules	Amgen Inc.
Thomas Stidham	Texas Health
Scott Stuewe*	DirectTrust
Rob Suarez	CareFirst BlueCross BlueShield
Bezawit Sumner*	CRISP Shared Services
Roisin Suver*	Humana Inc.
Brantley Synco	SS&C Technologies
Russell Teague	Fortified Health Security
Matthew Webb	HCA Healthcare
Tim Witos	McKesson
Axel Wirth*	MedCrypt
Nathalie Yarkony	U.S. Food and Drug Administration
Bill Yurick*	HHS Centers for Medicare & Medicaid Services