



Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Coordinating Council Cybersecurity Working Group

Health Industry Cybersecurity

SECTOR MAPPING AND RISK TOOLKIT – (SMART)

SMART Overview

Context

- **Technology systems are more complex and interconnected than ever before**, as a result of further integration and M&A activity
- **Cyberattacks on third party systems** introduce ever-expanding risk to the healthcare sector
- **This initiative developed an assessment of systemic risks in healthcare services** brought on by cyber incidents to core technology systems
- **IN SCOPE:** *Third party systems, entities, and processes in the healthcare sector where prolonged outages from a cyber incident could result in material sector-wide impacts*
- **OUT OF SCOPE:** IT infrastructure (e.g., cloud services providers, datacenters), dependencies on other critical infrastructure (e.g., water, gas, power), and software design

Objectives

- **Identify chokepoints in the healthcare system** that could impact the flow of information, payments, or medical services for core healthcare delivery and ancillary functions material to the functioning of the sector
- **Risk assess clinical, administrative, and financial impacts** of cybersecurity incidents against third party services and technology in critical health system work flows ensuring that organization is focused on only those vendors and risks material to the organization.
- **Mitigate identified risk for critical vendors** ensuring that that the most resources and effort are engaged on the riskiest vendors that present the highest material risk to the organization.
- **OUTCOME: Organizations will spend 80% of their time mitigating the highest risk to the organizations and only 20% of their time assessing risk, instead of the inverse.**

High Level Approach

- **Identify most material workflows and functions across healthcare sector based on the following criteria where there are workflows and systems that:**
 - Carry and/or transmit the most electronic health information or other protected information (PII, trade secrets, etc)
 - Transmit claims, payments and payment information flow
 - Have concentration risk where there are only one or two vendors that provide more than 90% of the solution to the sector.
 - If failure occurred, there would be significant and widespread impact to multiple sub-sectors within healthcare
- **Create process flow charts on prioritized functions to identify entire process flow and potential chokepoints**
- **Create risk assessment framework for individual organizations to identify and quantify their specific risks**
- **Recommend mitigations for residual vendor risk after assessment is complete.**

SMART Initiative Process 2024-25

- **Scope** - Scoping process began at HSCC Cybersecurity Working Group All-Hands membership meeting with HHS in Washington DC April 2024 following Change Healthcare incident
- **Organize**- Sector Mapping And Risk Template (SMART) Task Group kicked off October 2024
- **Convene** - SMART TG consisted of more than 80 health sector executive members, including CISOs, CIOs, Risk Officers and their teams
- **Draft** - Weekly zoom meetings with screen editing of maps; Drafts refined and validated by workflow management inside participating organizations
- **Workshop** - Additional workshopping of workflow maps during November 2024 and April 2025 All-Hands meetings
- **Assemble and Finalize**– Final drafting of usage guidance toolkit and map formatting through the summer, published October 2025, with full maps under controlled distribution for “need to use” stakeholders in healthcare system

Core Healthcare Workflows Mapped

- Map 1 Blood
- Map 2 Claims and Payments
- Map 3 Dialysis
- Map 4 EMS
- Map 5 Home Health
- Map 6 Laboratories
- 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
- Map 11 Public Health Strategic National Stockpile
- Map 12 Public Health Surveillance
- Map 13 Public Health Vaccines-Children
- Map 14 Public Health Vaccines-Pandemic
- Map 15 Radiology-Diagnostic
- Map 16 Radiology-Therapeutic
- Map 17 Retail Pharmacy

Full Maps are available to vetted qualified users by request at

<https://healthsectorcouncil.org/workflow-maps-request>



Maps are TLP/RED – do not share them outside your organization

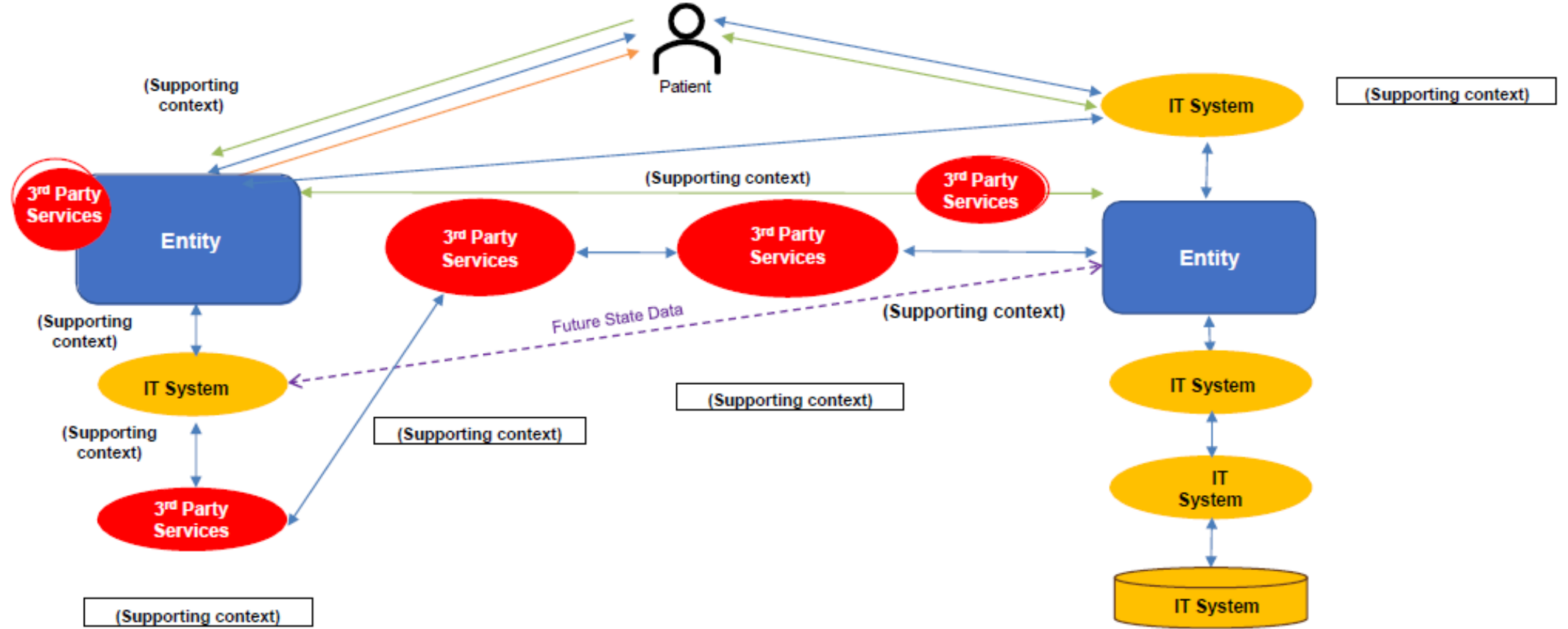


Example Maps (Redacted)

Full Maps are available by request at <https://healthsectorcouncil.org/sector-risk-mapping>

Full Maps are **TLP/RED** – do not share them outside your organization!

Commercial Medical Claims and Payments

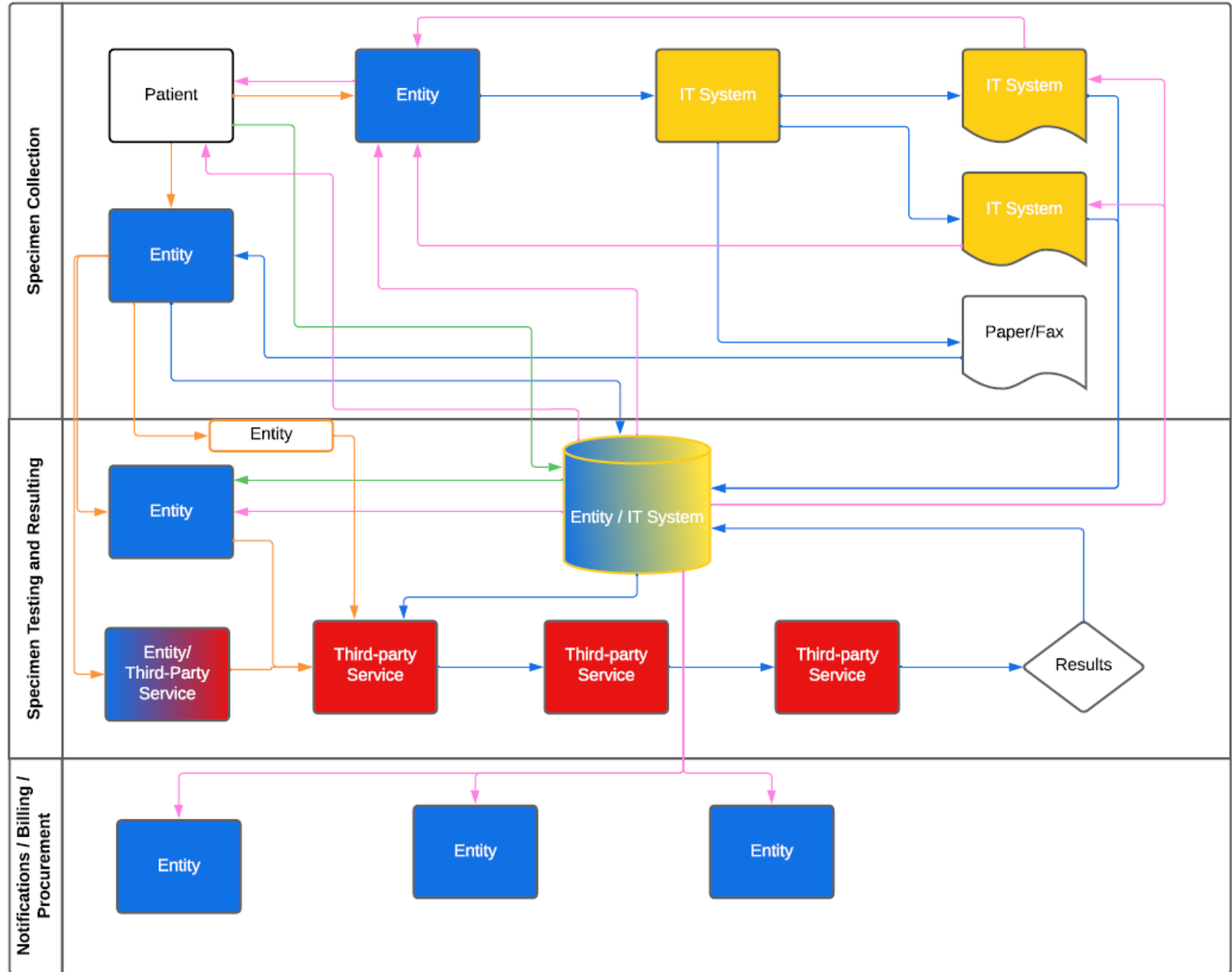


LABORATORIES MAP

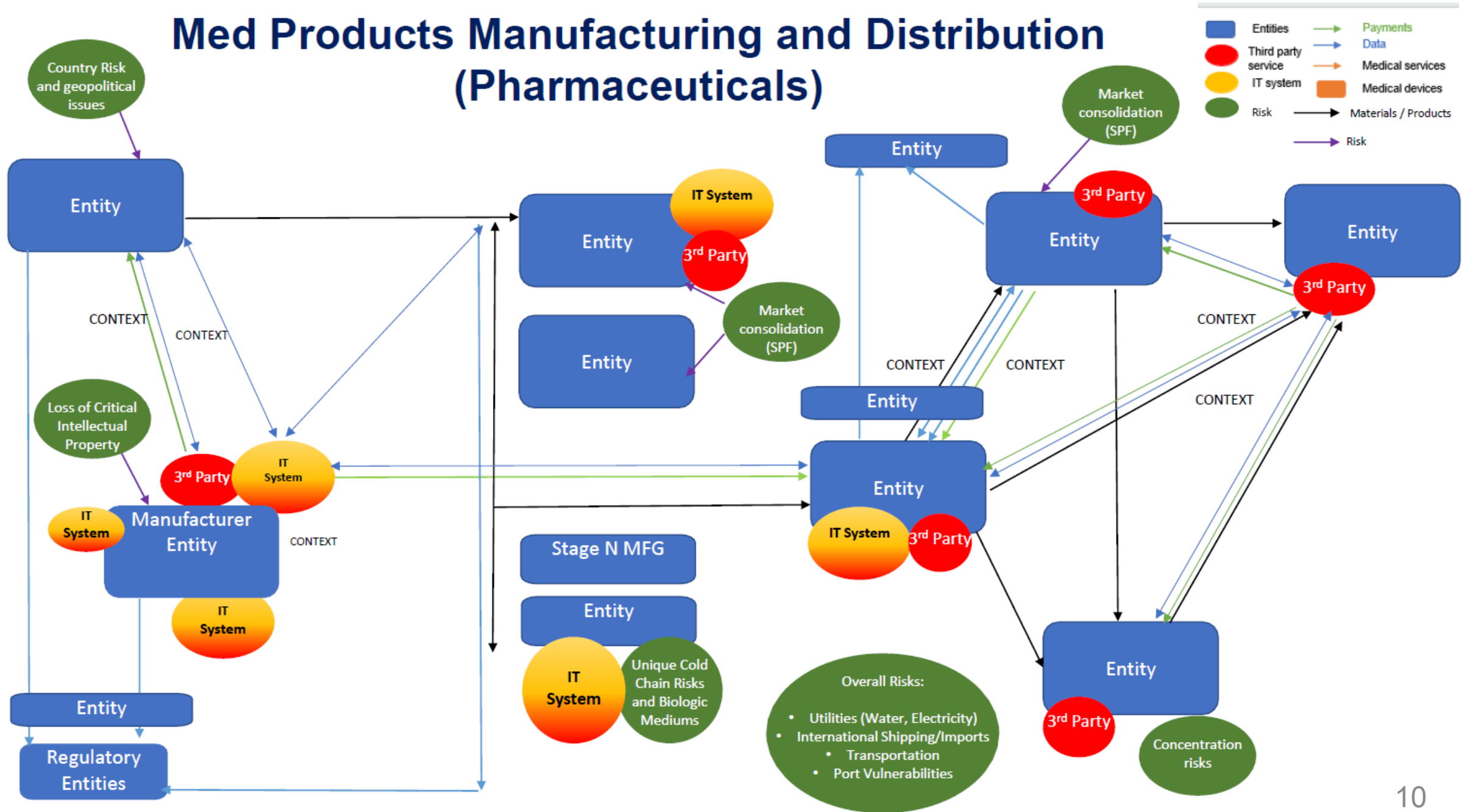
Line Key



Shape Key



Med Products Manufacturing and Distribution (Pharmaceuticals)



Initial Findings

Topic

Cross-cutting challenges

- **Resiliency against cyber attacks, especially third-party attacks, requires operational redundancies** (which can be technological such as multiple claims clearinghouses or manual such as downtime workarounds)
- **Lack of visibility among all relevant parties** on IT vendors that run “plumbing” of healthcare system and among both healthcare leadership (providers, payers, etc.) and technical staff on internal systems and processes
- **Increased reliance on outsourced services, coupled with workforce capacity challenges**
 - Driving investments into remote medical and administrative services that expand the scope of third-party operations, thus driving risk (e.g., outsourcing and offshoring billing and coding, nighthawk radiology services)
 - Corresponding workforce reductions curbing potential manual workarounds that require staff for execution
- **Healthcare industry shifting to more cloud-based services, improving overall security but also consolidating chokepoints** to major cloud vendors and software-as-a-service operations; lesser resources exacerbate challenges

Function-specific insights

- **Concentration risks prevalent across key functions; e.g., e-prescribing, reference labs, therapeutic radiology, etc.**
- **Large electronic health records vendors typically operate on local networks**, but system downtimes for cloud-hosted services can cascade across clients’ systems, impacting downstream providers
- **Various mid-market vendors control cloud-based host environments of numerous services** (e.g., EHR, billing/coding, eligibility verification, etc.) for smaller organizations, creating additional vulnerability for subscale providers
- **Payer dependencies (e.g., billing and coding services, clearinghouse) are pervasive across sector**, and risks are most acute for smaller organizations in light of lesser redundancies and capacity; however, no major consolidation in medical billing and coding
- **Reference labs present two risks – i) concentration risk, though less magnified given volume other players (private labs, academic labs, state labs, etc.); ii) need for additional review of cloud hosted middleware solutions**, which are leveraged by large reference labs to connect diagnostic equipment with third party analyzer systems and lab information systems

Lesser vulnerabilities

- **Devices and patient monitoring systems (e.g., catheterization labs, dialysis systems, etc.) do not rely on third party services to operate but may for ongoing support**; disruption to these systems may only be localized
- **Radiology information systems, image data systems (i.e., PACS), and radiology interpretation tools are generally hosted locally and offline PACS systems do not impact ability to use radiology devices**; and no dependency on middlemen for data exchange in radiology due to common data standard (DICOM); however, growing consolidation in teleradiology may be a concern and downtime plans for remote reading of images does need to be developed and implemented at all locations.

Next Steps (For Users)

- **Download the Final Guidance Document**
- **Apply The Risk Assessment Process to Your Specific Organization**
- **Develop priority list of high-risk vendors that additional mitigations are needed**
- **Start focusing on mitigation of those vendors to reduce systematic risk in your organization**
- **Provide feedback on maps and process to HSCC for future refinements of process and additional sector wide insights**

Appendix

Risk Assessment Summary (1/3)

Functions

Key third party IT services

Risk assessment summary

Medical claims

Medical clearinghouse

- Cyber incidents are exacerbated by a highly concentrated market coupled with exclusivity arrangements; small providers/hospitals disproportionately impacted
- Lack of planned redundancy coupled with technical burden to implement workarounds leads to longer term (e.g., 2-4 weeks) impacts on small providers

Eligibility verification systems

- Some eligibility services integrated with EHRs and other functions. More information needed to develop assessment

Retail pharmacy

Pharmacy switch

- Three dominant organizations mean disruption to pharmacy switch operations would significantly impact the ability for patients to receive medication
- Independent pharmacists often do not have an option to choose their switch vendors because their pharmacy management system vendor decides

E-prescribe

- E-prescribing highly concentrated, posing significant systemic risk with few alternative technical options for redundancy

Laboratory

Lab information systems

- Cyber incidents on two top reference lab information systems would significantly impact ability to send and receive lab results and may impact flow of blood products
- Cloud hosted middleware that connects analyzer systems to diagnostic equipment and lab information systems could pose systemic risks; more information needed

Middleware

- More information needed to assess prevalence and systemic security risks of middleware in reference labs

Analyzer tools

- More information needed on specific analyzer tools and software leverage for common lab tests

Risk Assessment Summary (2/3)

Functions

Key third party IT services

Risk assessment summary

Diagnostic Radiology

PACS & Radiology information systems

- PACS and radiology information systems generally hosted locally and have few or no middlemen for data exchange due to the common data standard (DICOM)
- Disruption to PACS would be localized and local downtime reading plans are needed
- General trend towards cloud based PACS and outsourcing of radiology services

Interpretation tools

- Radiology interpretation tools are generally hosted locally, posing limited systemic risk across the sector until widespread adoption of AI
- Use of third-party AI tools will increase over time, introducing new risks but more information needed to map impacts

Therapeutic Radiology

- Rely on Diagnostic Radiology flows and transmits data to cloud hosted treatment planning solutions which are concentrated with two major vendors. Any major disruption in treatment planning vendors would cause significant disruption to sector.
- Use of third-party AI tools will increase over time, introducing new risks but more information needed to map impacts

Other Critical Flows

Supplies and Pharmaceuticals

- Reliant on several manufacturing and compounding steps both onshore and offshore which can impact availability because of concentration risks.
- More information needed to assess systemic impacts of incidents on third party services as most health systems rely on one large distributor for supplies/pharma

Blood

- Reliant on Laboratory workflows and therefore extended lab downtime in concentration vendors may significantly impact blood availability.
- Regional and state level concentrations of vendors posing local risks.
- Regional and State Laws and regulations will also play a role in use and availability of blood products during downtime events.

Risk Assessment Summary (2/2)

Functions

Key third party IT services

Risk assessment summary

Other Critical Flows

Outpatient Dialysis

- Concentration risk of Outpatient Dialysis vendors across the sector could lead to significant sector impacts if one of those vendors is compromised.
- More information needed to assess systemic impacts of incidents on third party services that collect and transmit data that contributes to treatment decisions

Emergency Medical Services

- Solutions may run locally and are not dependent on a single concentrated third-party service to operate, however systematic impacts from outages of telephone, power or other critical infrastructure systems may compromise the function.

Electronic health records

- Small and rural health centers often use vendors that bundle services like EHR, billing and coding, eligibility verification, and patient interfaces, consolidating critical dependencies to one vendor
- Cloud based EHR services from larger vendors can pose widespread systemic risks

Medical devices

- Devices run locally and are not dependent on third party services to operate, but may be for support and certificate updates.
- More information needed to assess systemic impacts of incidents on third party services that collect and transmit data that contributes to treatment decisions

Billing and coding

- Billing and coding dependencies are pervasive across healthcare system, however there is no major consolidation
- Organizations leverage a variety of sources (e.g., outsourcing to third parties, offshoring, etc.)

Key enablers

Discussion

Connect

SMART Toolkit

<https://HealthSectorCouncil.org/SMART-Toolkit>

More Information

<https://HealthSectorCouncil.org/Contact>