It Takes a Village:

A Team-Based Approach to Clinical Cybersecurity

Katie Adams, MHA, PMP

Steve Ellithorpe, CHTM, CBET

Mike Ratliff, CISSP, CISM

Annual Conference 2024

Building the Future of Health Together

Presenters

Katie Adams, MHA, PMP

Clinical Cybersecurity Director
Providence

Steve Ellithorpe, CHTM, CBET

Executive Director, Clinical Technology
Strategy & Innovation, Providence

Mike Ratliff, CISSP, CISM

AVP, Security Engineering & Operations
Providence

Agenda

- Learning Objectives
- Background
- Clinical Cybersecurity Journey
  - Our Approach
  - Key Stakeholders
  - Process Improvements
  - Useful Tools
- Barriers & Challenges
- Outcomes & Key Results
- Takeaways & Lessons Learned
- Q & A

Learning Objectives

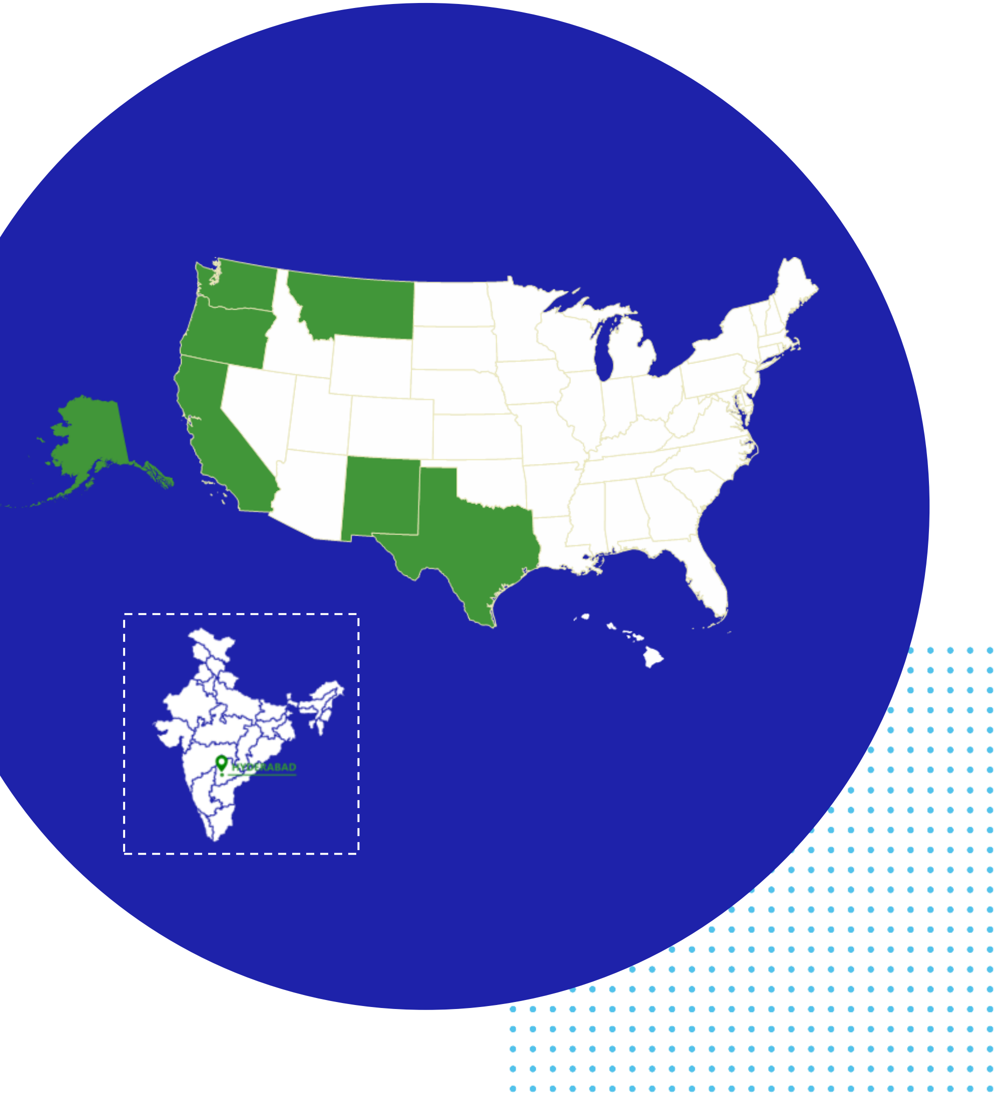
At the end of this session, participants will be able to:

1. Define a team-based approach to clinical cybersecurity.
2. Describe the importance of collaboration and ownership to the success of a clinical cybersecurity program.
3. Choose stakeholders required for effective implementation of a clinical cybersecurity program.
4. Analyze various tools to support enhanced visibility of network-connected clinical devices.
5. Evaluate processes to improve medical device procurement and shorten organizational response time for clinical cybersecurity incidents.

Background

- Who is Providence?
- Why create a Clinical Cybersecurity program?
- Our Journey

Who is Providence?



122K
Caregivers

38K
Nurses

34K
Physicians

$2.1b
Community Benefit

51
Hospitals

1000
Clinics

29m
Total Patient Visits

2.6m
Covered Lives

1700+
Published Research Studies

1
Health Plan

18
Supportive Housing Facilities

High School, Nursing Schools & University

1200
Volunteer Governance Members

Why Create a Clinical Cybersecurity Program?

Globally, healthcare remains one of the most frequently-targeted industries for cyber attacks due to:

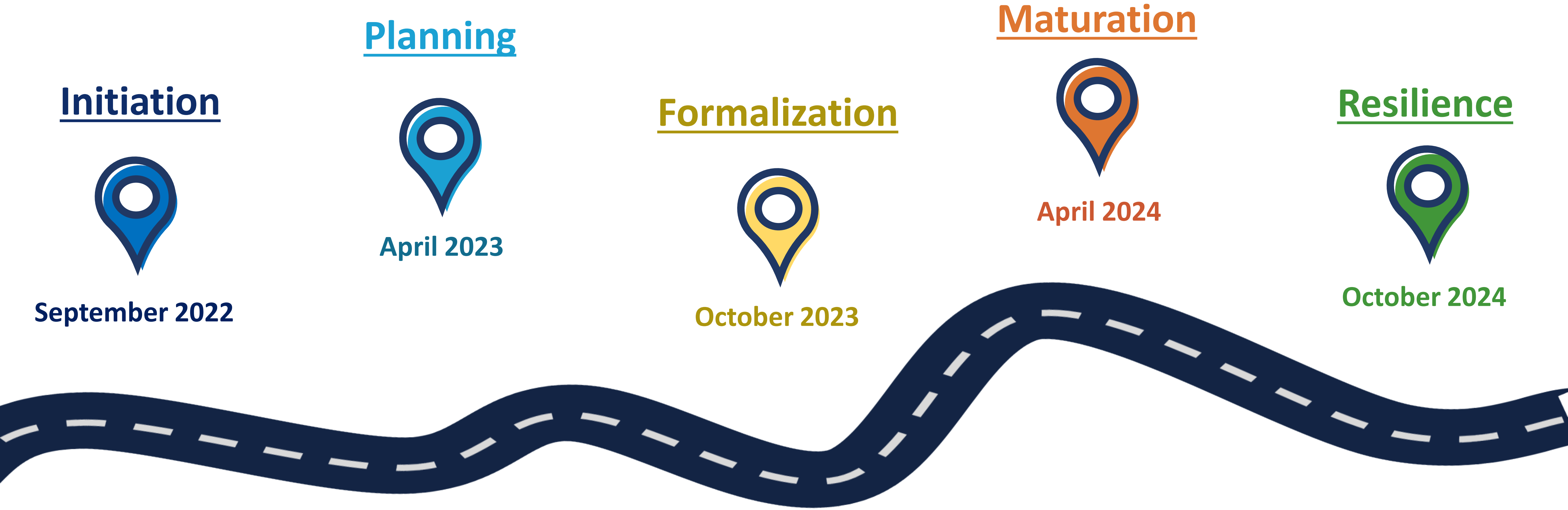
- Vulnerable devices (especially medical devices…)
- Valuable patient information (PHI, PII…)
- Very critical to national infrastructure
- Virtual entry points (VPNs...)
- Vast technical debt

Why Create a Clinical Cybersecurity Program?

Internally, we recognized a need to…

- Decrease cyber incident response time.
- Reduce misunderstandings between teams about their roles and interdependencies.
- Improve and streamline the procurement and onboarding of new clinical devices.
- Evolve the traditional “IT” approach to managing technical debt and security for clinical devices.
- Unite as a team to solve these challenges.

Our Clinical Cybersecurity Journey



Initiation

September 2022

Planning

April 2023

Formalization

October 2023

Maturation

April 2024

Resilience

October 2024

STEP 1

Program Initiation

KEY ACTIVITIES:

- Define program scope
- Establish common language & goals
- Develop device criticality classifications & governance principles

Clinical Cybersecurity Program Scope

We established this program to:

- ✓ Develop a common language to identify and discuss distinct types of clinical and medical devices.
- ✓ Create a Clinical Cybersecurity team responsible for enhancing the security of clinical devices.
- ✓ Deploy a standard set of tools to enhance visibility of network-connected clinical devices.
- ✓ Collaborate to align clinical device lifecycle and procurement roadmaps.
- ✓ Improve the medical device procurement processes.
- ✓ Set realistic goals and measure progress toward these accomplishments.

Bringing the “Villages” Together

Establishing a Common Language

(Some) Examples:

- Patch vs. Update vs. Upgrade
- Medical Device vs. Clinical Device
- Compute Device vs. Application
- Workstation vs. Workstation
- Incident vs. Service Request

Monitor

vs

Monitor

Incident Response Methodology by Device Type

Definition:
Device is essential to operations. We cannot function without it. Could cause physical harm to patients if interrupted.

Incident Response: Device cannot be pulled off network without consent from device owner.

Examples:
Interventional procedures, HVAC system, Life Support Equipment, HUGS, Fetal Monitoring

Definition:
Significant impact to operations, patient care, and clinical workflows if interrupted, but cannot cause physical harm to patients. Includes regulated devices only. Workaround requires additional staffing.

Incident Response:
Notify owner first, then pull device off network.

Examples:
Imaging Devices (MRI, CT, Xray), Pyxis, Nurse Call

Definition:
Devices supporting patient care with least disruption to patient care and clinical workflows if impacted. Includes regulated and non-regulated devices.

Incident Response:
Pull device off network, then immediately notify owner.

Examples:
PACS, Middleware, Data Aggregators

Definition:
Devices not directly supporting the delivery of patient care.

Incident Response:
OK to pull from network and then deliver automated notification per SLAs.

Examples:
WOWs, Nurse Workstations, Caregiver laptops

"Compute Devices/ Corporate IT"

"Medical Devices" **"Clinical Devices"**

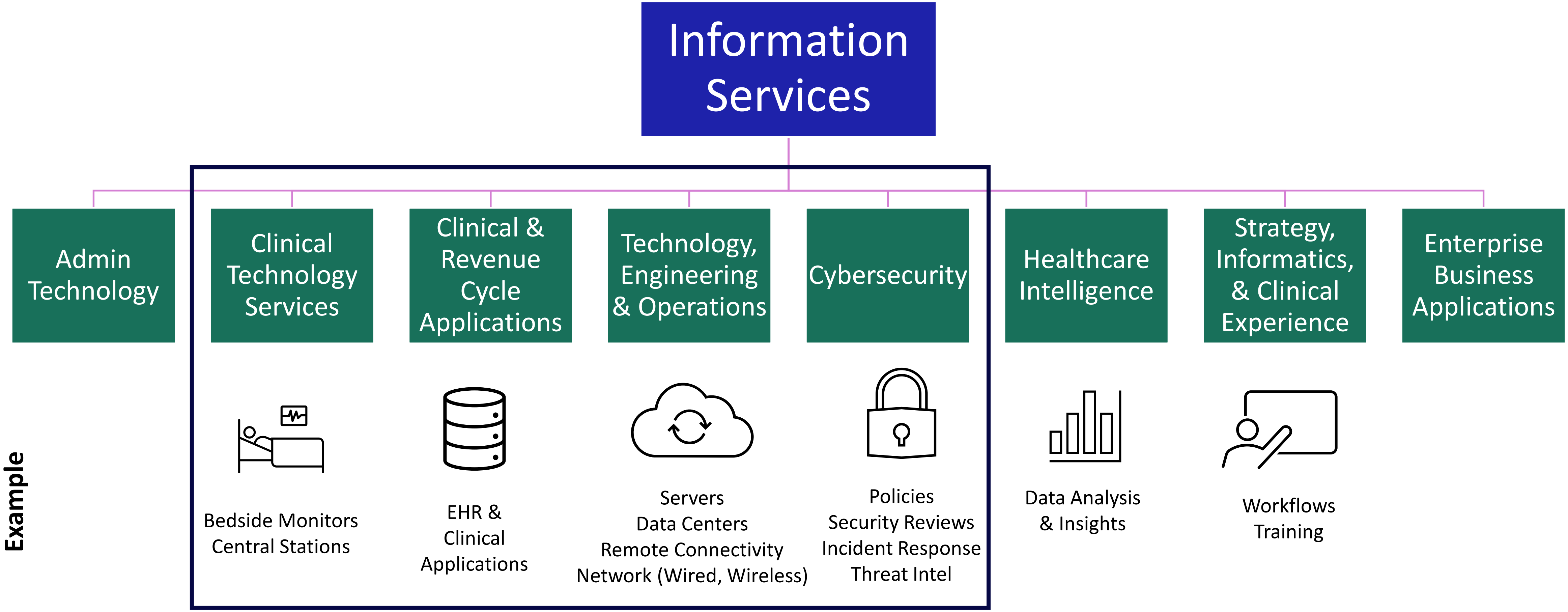
STEP 2

Program Planning

KEY ACTIVITIES:

- Engage stakeholders
- Understand current state
- Utilize tools to prioritize the work

Key Stakeholders – IS Teams



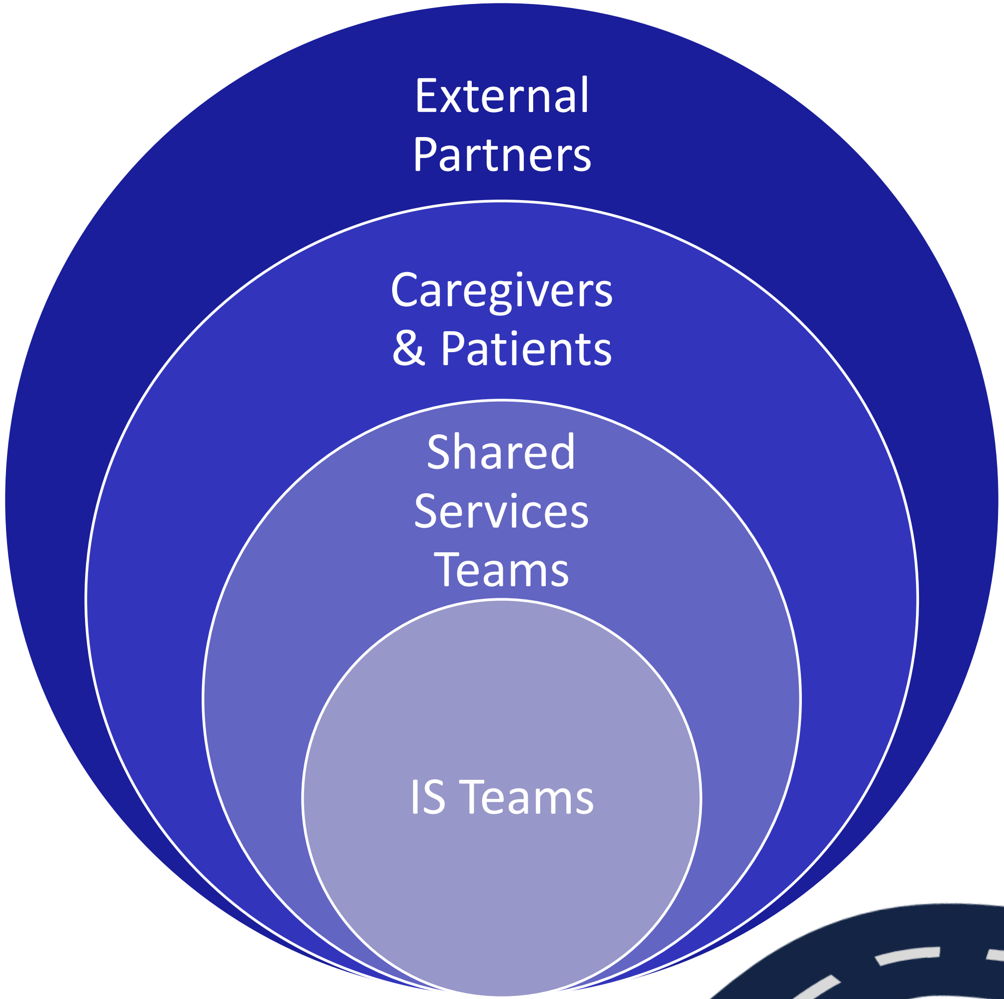
Information Services

- Admin Technology
- Clinical Technology Services
- Clinical & Revenue Cycle Applications
- Technology, Engineering & Operations
- Cybersecurity
- Healthcare Intelligence
- Strategy, Informatics, & Clinical Experience
- Enterprise Business Applications

Patient Monitoring Example

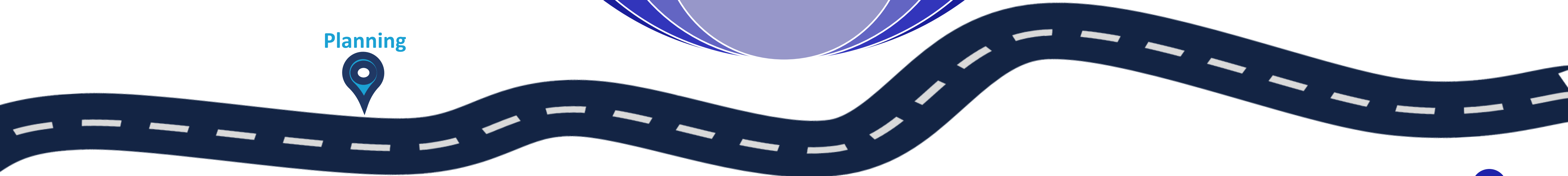
Clinical Technology Services	Clinical & Revenue Cycle Applications	Technology, Engineering & Operations	Cybersecurity	Healthcare Intelligence	Strategy, Informatics, & Clinical Experience
Bedside Monitors Central Stations	EHR & Clinical Applications	Servers Data Centers Remote Connectivity Network (Wired, Wireless)	Policies Security Reviews Incident Response Threat Intel	Data Analysis & Insights	Workflows Training

Key Stakeholders – Beyond IS Teams (It Takes a Village)



External Partners
Medical Device Vendors
Other Health Systems
Consultants

Shared Services Teams
Purchasing / Contracting
Risk Management
Finance



Understanding the Current State & Prioritizing our Work

Tools used:

- Centralized asset management database (Inventory)
- Anti-malware & vulnerability management software platforms (Security)
- Deep-packet inspection tools to identify network-connected clinical devices (Network)

Opportunities for improvement:

- Remediate Technical Debt
- Improve Procurement Processes
- Streamline Technology Reviews
- Enhance Incident Response
- Strengthen Vendor Management
- Increase Understanding & Awareness

STEP 3

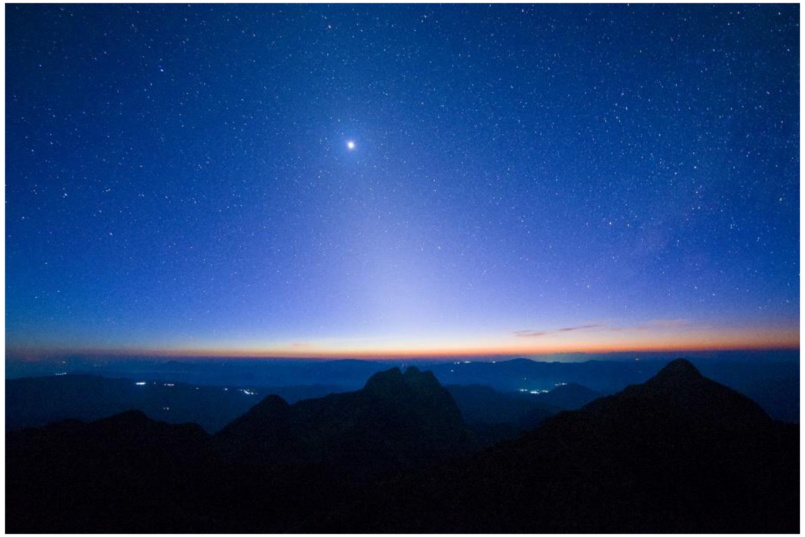
Program Formalization

KEY ACTIVITIES:

- Establish guiding principles
- Create data alignment & transparency
- Maintain cross-functional collaboration

Our Guiding Principles

- Prioritizing **clinical** requirements in a **secure** cyber culture
- Medical devices are **not** IT devices
- IT does **not** make clinical decisions
- Focus on the **people**, not the “stuff”
- Processes need to move at the **speed** of business



Aligning our Data

Goal

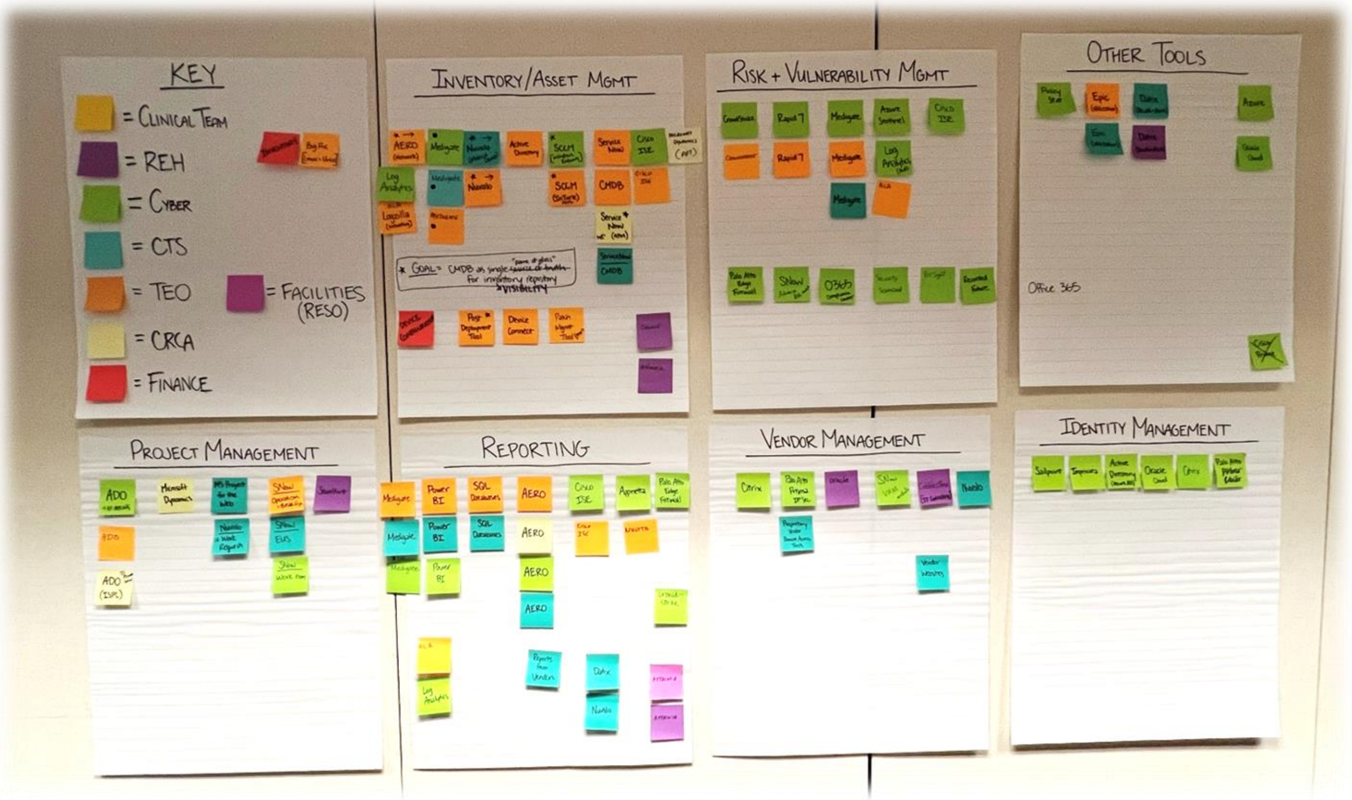
- Ensure data accuracy and visibility across the organization

Considerations

- What data sources do our teams currently rely on? For what purposes?

Solution

- Master Data Management Console *(work in progress)*



Formalization

The Collaboration Continues…

- Setting common goals and metrics.
- Implementing a variety of projects and process improvements to achieve stated goals.
- Checking-in regularly to maintain alignment across teams.
- Educating others about the importance of clinical cybersecurity.
- Gathering feedback from stakeholders.
- Proactively planning for the future.

STEP 4

Program Maturation

KEY ACTIVITIES:

- Establish a Vendor Management Council
- Implement Regular Business Reviews
- Improve Cyber Incident Response Processes

Vendor Management Council

Strategic Goals

- Support cross functional teams to provide input necessary to make informed decisions through a streamlined, consistent and transparent review process for all strategic vendors.
- Create a collaborative forum to align on vendor strategies, incident response and technology onboarding.

Chair
REH Director

General Manager
REH Team Member

Membership:
Functions Represented

- Clinical & Revenue Cycle Applications (CRCA)
- Cybersecurity
- Clinical Technology Services
  - IS Field Services
  - Clinical Engineering
- Technology Engineering & Operations (TEO)
  - Network
  - Endpoint
  - Server
- Resource, Engineering & Hospitality (REH)
  - Equipment Strategy & Planning
  - IT Contracting

Scope

Focus Areas

1. Develop and maintain standard business process flows in collaboration with cross-functional teams
2. Communicate SME feedback to appropriate Clinical Councils, in particular risks and key operational considerations for medical equipment, that will inform current or future decisions
3. Balance vendor requirements with IS requirements: Allow for a venue to document vendor issues while ensuring appropriate actions and remediations are taken
4. Ensure visibility of organizational standards to carry out teams' independent strategic initiatives
5. Act as a resource for business/operational leaders to consult on upcoming RFPs and strategic initiatives to designate appropriate stakeholders and share organizational risks, and other system-wide implications.

Scope

- Performance management of medical equipment vendors
- Quarterly business reviews for top 5 collaborative clinical/technology vendors
- Review vendor rules of engagement
- New technology; how it will impact current standards

Interdependencies

- Interdependence with Clinical Councils and Division Executive Leadership

Vendor Management Scorecard (Business Reviews)

Focus areas include:

- ✓ Mission
- ✓ Account Support
- ✓ Contract Management
- ✓ Innovation
- ✓ Collaboration
- ✓ Compliance
- ✓ Service Quality
- ✓ Cybersecurity
- ✓ Technology

Cyber Incident Response Planning

- Identify device locations & ownership
- Establish an incident command structure
- Develop a robust communications plan
- Prepare for the worst-case scenario
- Implement redundancies
- Conduct regular tabletop exercises
- Debrief to improve processes
- Repeat

Maturation

STEP 5

Program Resilience

KEY ACTIVITIES:

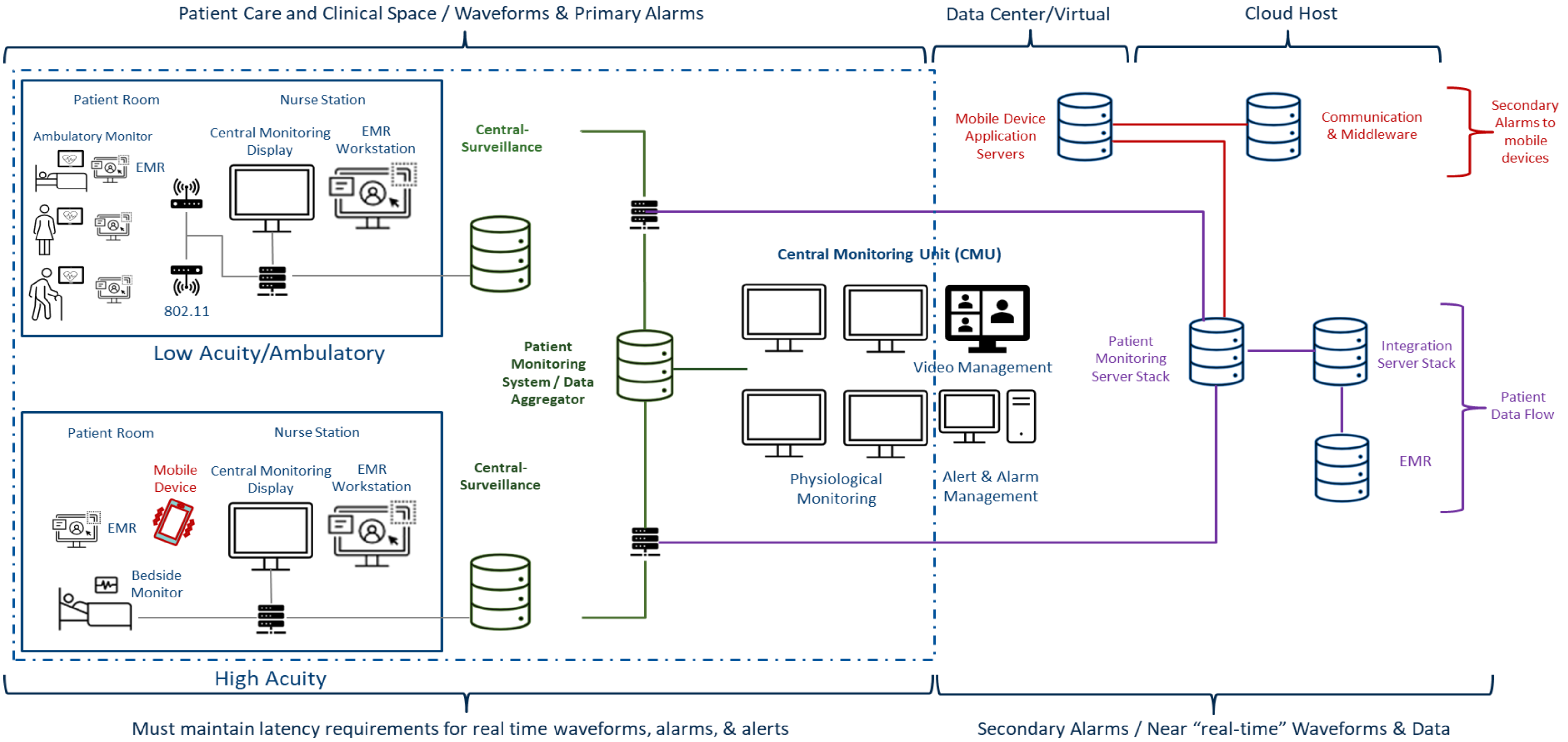
- Improve Device Procurement Processes
- Develop Standard Reference Architecture
- Establish Ongoing Support Models

Program Resilience & Sustainability

This work drives the future of healthcare!

- Bring awareness to process gaps & define impact
- Communicate about cybersecurity & technical debt
- Establish device standards & reference architecture
- Build an “end-to-end” procurement process
  - Medical Device standards
  - Infrastructure & Integration standards
  - Aligned with contractual obligations
- Prepare to educate & be educated; rinse & repeat

Reference Architecture - Standard Configuration & Deployment


Patient Care and Clinical Space / Waveforms & Primary Alarms
Data Center/Virtual
Cloud Host
Patient Room
Nurse Station
Ambulatory Monitor
Central Monitoring Display
EMR Workstation
EMR
802.11
Low Acuity/Ambulatory
Central-Surveillance
Patient Monitoring System / Data Aggregator
Central Monitoring Unit (CMU)
Video Management
Physiological Monitoring
Alert & Alarm Management
Mobile Device Application Servers
Communication & Middleware
Secondary Alarms to mobile devices
Patient Monitoring Server Stack
Integration Server Stack
EMR
Patient Data Flow
Patient Room
Nurse Station
Mobile Device
Central Monitoring Display
EMR Workstation
EMR
Bedside Monitor
Central-Surveillance
High Acuity
Must maintain latency requirements for real time waveforms, alarms, & alerts
Secondary Alarms / Near "real-time" Waveforms & Data

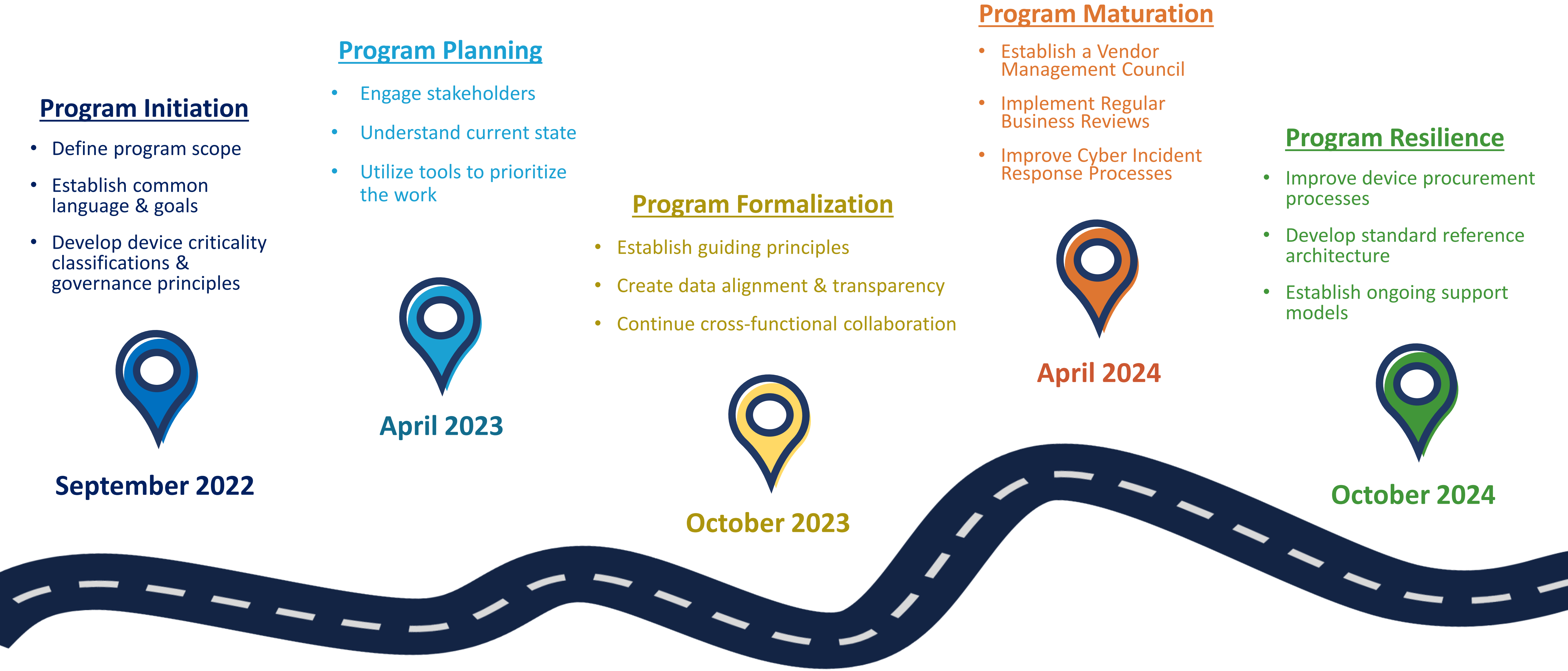
Procurement & Support Models

Stakeholders / Teams	Healthcare Environment		
	Pre-Purchase / Pre-Deployment	Clinical Care Area / Deployed	Technical & Infrastructure / Post-Deployment
Infrastructure - Network (TEO)	✓ Design ✓ Engineering ✓ Standards Development ✓ Policy Requirements ✓ Security Assessment ✓ Design Review ✓ Integration Alignment ✓ Installation Planning ✓ Deployment Timing ✓ Clinical Operation ✓ Patient Care Standards ✓ Caregiver Education ✓ Contract Negotiation & Management	• Installation • Scheduled Maintenance • Service Response • Knowledge Base • Caregiver Operational Support • Caregiver Education • Security Patching • System Updates • Device Upgrades • Documentation • Regulatory Compliance • Decommission (Core services Clinical Engineering delivers to the Organization) • Applications & Infrastructure • Outcomes or Usage	▪ SOP = Monitoring (network & infrastructure health) ▪ Cybersecurity ▪ Security Patching ▪ Support Tools ▪ Upgrades ▪ Decommission ▪ Installation ▪ Service & Service Response ▪ Security Patch ▪ Updates ▪ Upgrades ▪ Knowledge Base ▪ Documentation ▪ Decommission
Infrastructure – Workstation Engineering (TEO)			
Data Infrastructure - Servers (TEO)			
Cybersecurity / Security Operations			
Clinical Applications (Integration)			
Clinical Applications (Clinical Apps)			
Clinical Engineering			
End User Support			
Clinical Stakeholder			
Regulatory			
REH / Contracting / Legal (Purchase Agreements)			

Summary

- Barriers & Challenges
- Outcomes & Key Results
- Takeaways & Lessons Learned

Providence’s Clinical Cybersecurity Journey



Program Initiation

- Define program scope
- Establish common language & goals
- Develop device criticality classifications & governance principles

September 2022

Program Planning

- Engage stakeholders
- Understand current state
- Utilize tools to prioritize the work

April 2023

Program Formalization

- Establish guiding principles
- Create data alignment & transparency
- Continue cross-functional collaboration

October 2023

Program Maturation

- Establish a Vendor Management Council
- Implement Regular Business Reviews
- Improve Cyber Incident Response Processes

April 2024

Program Resilience

- Improve device procurement processes
- Develop standard reference architecture
- Establish ongoing support models

October 2024

Barriers & Challenges

- Initially underestimating the complexity of medical devices.
- Navigating Providence’s size and complexity to scale the work and move with speed.
- Balancing competing priorities, including technology, risk, and clinical operations.
- Addressing IT knowledge gaps related to medical device capabilities.
- Difficulties collaborating with 3rd party vendors.

Outcomes & Key Results

To date, our Clinical Cybersecurity program has:

- ✓ Remediated over 11,000 medical devices.
- ✓ Completed 3 separate patching pilots with different types of medical device modalities across various Providence geographic locations.
- ✓ Implemented a standardized cybersecurity risk identification tool, as well as an enterprise-wide inventory management tool.
- ✓ Improved cyber incident response time for clinical devices from hours to minutes.
- ✓ Increased engagement with key vendor partners through regular business reviews.

Takeaways & Lessons Learned

- **Establishing a common language is key to success.** It is important for everyone to be on the same page about the various device definitions to reduce confusion and ensure shared understanding and alignment.

- **Clinical cybersecurity cannot happen in a silo.** It is important to utilize a team-based approach and build trust to drive the successful execution of a clinical cybersecurity program.

- **Medical devices cannot be approached the same way as traditional IT devices.** Due to their complex nature and interdependencies with direct patient care, changes to medical devices must be implemented with an abundance of caution to avoid negative impacts to patient care and operations.

- **Clinical cybersecurity is a dynamic space.** Rapidly changing requirements and other challenges require the creation of a flexible program structure that is easily adaptable to change.

- **It is okay to ask for help.** Collaboration with a wide range of internal and external stakeholders is critical for the development of a successful clinical cybersecurity program based on industry best practices.

Questions?

Speaker Contact Information

Providence

Katie Adams, MHA, PMP

Clinical Cybersecurity Director
Providence

katherine.adams@providence.org

Steve Ellithorpe, CHTM, CBET

Executive Director, Clinical Technology
Strategy & Innovation, Providence

stephen.ellithorpe@providence.org

Mike Ratliff, CISSP, CISM

AVP, Security Engineering & Operations
Providence

michael.ratliff@providence.org

Thank You