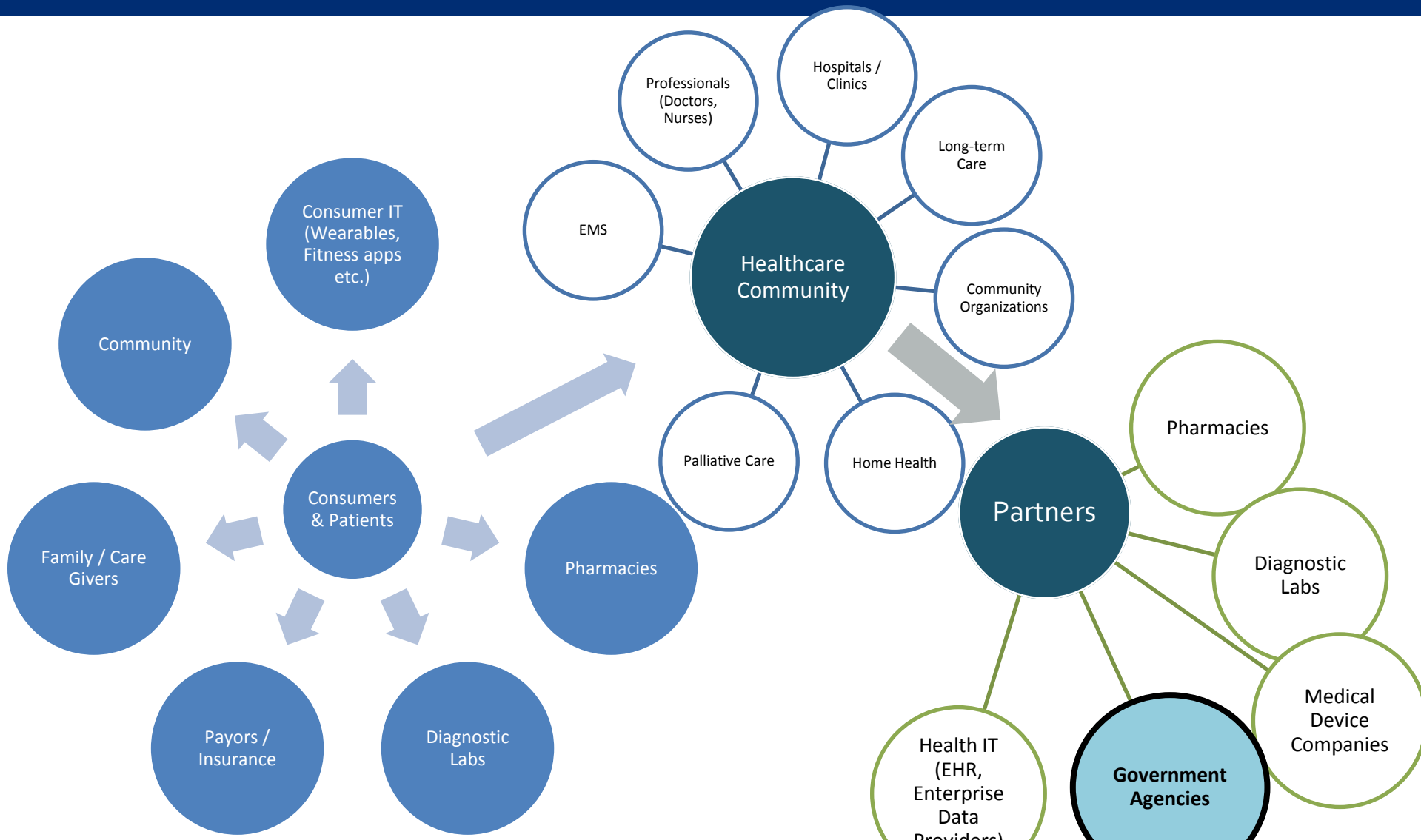
NEW YORK STATE | Department of Health

Protecting our Connected landscape

And promoting a culture of sharing…

Cyber Security

- Healthcare Cyber Security is in a state of transformation with electronic medical records and medical devices as integral components of delivering patient care.
- Comprehensive cyber security practices are essential to protect these digitally connected systems from disruption and to preserve the capacity of operations.
- As recent highly visible incidents have demonstrated, exploited system vulnerabilities in one location can lead to the rapid spread of damaging malware across interconnected networks and systems.



Healthcare ***CONNECTED*** *Eco system*

NEW YORK STATE Department of Health

Cyber – Risk Assessment

Healthcare facilities have greater responsibilities to secure their systems, medical devices and patient data to mitigate this risk.

The Security Management Process standard of the HIPAA Security Rule requires all covered entities and business associates to:

- **conduct an accurate and thorough risk analysis** of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI the entities create, receive, maintain, or transmit.
- **implement security measures** sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

HIPAA Security Rule Toolkit -- intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates https://scap.nist.gov/hipaa/

NEW YORK STATE | Department of Health

Assessing Risk – Cyber Events

Cyber attacks are insidious: very sudden, providing little or no warning

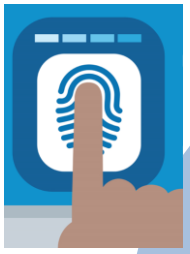
- Facilities may not even realize they've been attacked until long after it occurred.
- Cyber attack can cause patient harm and/or very severe and potentially extended disruption of services with costly recovery
- Hardening a facility for Cyber calls for a unique level of preparedness

Cyber attacks exploit fairly common vulnerabilities in the healthcare sector:

- Lack of staff and workforce trained in dealing with Cyber and network security
- Aging equipment, technology, software – running on outdated/not-supported operating systems; no security patches available
- Increasing number of internet connected devices
- Meaningful use incentives – drove "hyper-connectivity," rapid roll out with less concern for secure design; EHR access on patient internet connections

What steps can be taken by providers?

Focusing on the Basics



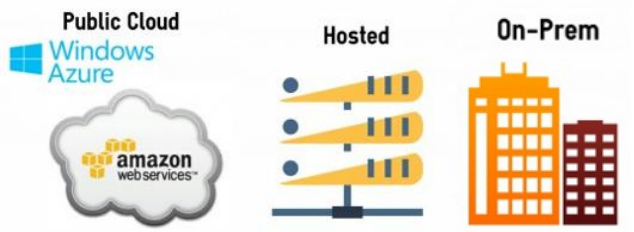
Who?

- Has access to our systems and data
- How are we managing access?

What external entities and data consumers we are working with?

Where?

- Are our systems located or hosted?



NEW YORK STATE Department of Health

Have a good response process

Incident Response Team

- Work together to make decisions based on the initial assessment
- Pre-defined roles, responsibilities, and contact information
- Assemble a virtual response team, if necessary

Reporting & Tracking

- Single system to report and track security incidents and ongoing updates
- Public Health Impact Assessment and Response

Breach Assessment

- Documented Notification Requirements (State, Federal and Law Enforcement)
- Engage cyber professionals for forensic and mitigation

Disaster and Contingency Planning

- Execute DR / COOP plans

NEW YORK STATE | Department of Health

Don’t hesitate to contact us

- Our interest is to learn about an event as early as possible.
- Assess Operational Impact and offer support.
- Encouraged by the coordinated response that we saw during the last few incidents.
- About three calls in total - First call lasted 30-45 min, then each 15 minutes

Sample Incident Report

Abbreviation key:
XYZ - Western Memorial Hospital
NNRC – Northeast Nursing & Rehabilitation Center

Area	Department	Issue	Status	Patient Impact
XYZ	Pharmacy	4/1/18: Loss of inventory control system, barcode scanners remain intact 4/2/18: Remain on critical override, 60% patched remotely with 40% requiring hands on, in progress today. 4/3/18 Scanner intermittent connectivity issues - Vendor on site to reimage and patch. Over 80% of all devices have returned to network. Remaining will remain on override.	In progress.	No impact.
XYZ	Medical Imaging MRI	4/1/18: Multiple vendors. Back online by noon up but some issues with quality. Off network, burning to disk at XYZ 4/2/18: In progress. Continuing to work off-network. 4/9/18: Fully Operational	In progress.	Patients rescheduled. Operational.
ER	Pharmacy	4/1/18: Computer down. Off network. Low-volume. Alternative method work-around continues. 4/2/18: Alternative method work-around continues. 4/3/18: Back on-line	In progress.	No impact.

Going forward

- Learning collaborative
- Joint exercise
- Ways to share and notify so that others can be vigilant