

Cybersecurity Threats and ALS Medical Devices

BOB JANUSAITIS, MPSA, CHLS, CISA, CISM, CRISC, CBCP, CESC

COMAL COUNTY ESD#2



SAFE-D

Texas State Association of Fire and Emergency Districts

Disclaimer

Audience survey

- How many have full time IT support for your cyber infrastructure?
- How many manage their IT infrastructure themselves?
- How many get County IT support?

Discussion items

- Emerging regulatory framework- HIPAA Cybersecurity Rule (proposed)
- The threat landscape
- Emerging technology
- What you can do to prepare

NEW HIPAA Rules

- [2024-30983.pdf](#)
- Comments by March 7, 2025 11:59pm EST: [Regulations.gov](#)



393 pages

← ↻ 🏠 <https://www.regulations.gov/docket/HHS-OCR-2024-0020> ☆ 🌐 ⚙️ | 📌 📄 ⋮ 📺

An official website of the United States Government. 🇺🇸

Regulations.gov
Your Voice in Federal Decision Making

[SUPPORT](#)

[← Back to Search](#)

R RULEMAKING DOCKET [Subscribe](#) [Share](#)

Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of ePHI

Created by the **Department of Health and Human Services**

[Open for Comments](#)

[Docket Details](#) [Unified Agenda](#) [Docket Documents 1](#) [All Comments on Docket 43](#)

✓ **Docket ID**
HHS-OCR-2024-0020

👤 **Number of Comments Posted to this Docket**
43
[More Details](#)

Summary ⓘ

This rule will propose modifications to the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). These modifications will improve cybersecurity in the health care sector by strengthening requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats.

[Give Feedback](#)

[Back to Search](#)

R RULEMAKING DOCKET

[Subscribe](#)

[Share](#)

Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of ePHI

Created by the Department of Health and Human Services

[Open for Comments](#)

[Docket Details](#)

[Unified Agenda](#)

[Docket Documents](#) 1

[All Comments on Docket](#) 43

REFINE RESULTS

☒ Only show documents open for comment (1)

Document Type

☐ Proposed Rule (1)

Posted

[Last 30 Days](#) (1)

[Last 90 Days](#) (1)

[Custom Dates](#)

Comments Due

[Next 90 Days](#) (1)

[Custom Dates](#)

SEARCH RESULTS

Search

[Open For Comment](#) x

[Clear Filters](#)

SORT BY [Comments Due \(Newer-Older\)](#)



PROPOSED RULE

Health Insurance Portability and Accountability Act Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Agency Department of Health and Human Services | Posted Jan 6, 2025 | ID HHS-OCR-2024-0020-0001

[Open for Comments](#)

[Comment Period Ends: Mar 7, 2025 at 11:59 PM EST](#)

[Comment](#)

Displaying 1 - 1 of 1 results




SAFE-D

Texas State Association of Fire and Emergency Districts

Proposed areas included in the new ruling

- Required specifications
- Written Policies, Plans, Analysis
- Network Maps & Asset Inventory
- Risk Analysis Assessment - \$\$\$
- Contingency Planning and Security Incidents
- Annual Security Rule Audits -\$\$\$
- Business Associate Verification
- Encryption Requirement
- Required Technical Controls and Safeguards
- Multi-Factor Authentication - \$\$
- Vulnerability Scans and Penetration Testing - \$\$\$\$

1 of 393

[BILLING N]  This document is scheduled to be published in the Federal Register on 01/06/2025 and available online at <https://federalregister.gov/d/2024-30983>, and on <https://govinfo.gov>

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office of the Secretary
45 CFR Parts 160 and 164
RIN 0945-AA22
HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

AGENCY: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking; notice of Tribal consultation.

SUMMARY: The Department of Health and Human Services (HHS or “Department”) is issuing this notice of proposed rulemaking (NPRM) to solicit comment on its proposal to modify the Security Standards for the Protection of Electronic Protected Health Information (“Security Rule”) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The proposals in this NPRM would increase the cybersecurity for ePHI by revising the Security Rule to address changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, “regulated entities”); other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.

Required specifications

- Previously, some things in the Security Rule were “addressable.” OCR wants to eliminate the distinction between “required” and “addressable” standards and make virtually all standards required.

Security Risk Assessment

Section 5 - Security and the Practice

Question #	Question Text	Indicator	Question Responses	Education	Risk Indicated	Required?	Reference
1	Do you manage access to and use of your facility or facilities (i.e., that house information systems and ePHI)?		Yes. We have written procedures in place restricting access to and use of our facilities.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.		Required	HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7 HICP: TV1 - Practice # 6
			Yes. Authorization of access to and use of our facilities is verbally communicated, but we do not have written procedures.	Consider implementing documented procedures to govern access to facilities. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.		Required	HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7 HICP: TV1 - Practice # 6
			No. We do not have a process to restrict access to our facilities.	Consider implementing documented procedures to govern access to facilities. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.		Required	HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7 HICP: TV1 - Practice # 6
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7 HICP: TV1 - Practice # 6
	Notes						
2	What physical protections do you have in place to manage facility security risks?		We have methods for controlling and managing physical access to our facility such as, keypads, locks, security cameras, etc. We also have an inventory of our practice's facilities that house equipment that create, maintain, receive, and transmit ePHI. Our policies and procedures outline managements' involvement in facility access control and how authorization credentials for facility access are issued and removed for our workforce members and/or visitors. Workforce members' roles and responsibilities in facility access control procedures are documented and communicated.	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks. Disable network ports that are not in use. Maintain network ports as inactive until an activation request is authorized. This minimizes the risk of an unauthorized user "plugging in" to an empty port to access to your network. In conference rooms or waiting areas, establish guest networks that separate organizational data and systems. This separation will limit the accessibility of private data from guests visiting the organization. Validate that guest networks are configured to access authorized guest services only.		Addressable	HIPAA: §164.310(a)(2)(ii) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 7, 16 HICP: TV1 - Practice # 6
			We have written procedures documenting our managements' involvement in facility access control procedures.	Ensure only authorized access to ePHI and facilities is allowed by implementing policies and procedures to limit physical access systems and facilities housing ePHI. Consider implementing policies and procedures to safeguard the facility and equipment from unauthorized tampering, theft, or physical access. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks. Disable network ports that are not in use. Maintain network ports as inactive until an activation request is authorized. This minimizes the risk of an unauthorized user "plugging in" to an empty port to access to your network. In conference rooms or waiting areas, establish guest networks that separate organizational data and systems. This separation will limit the accessibility of private data from guests visiting the organization. Validate that guest networks are		Addressable	HIPAA: §164.310(a)(2)(ii) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 7, 16 HICP: TV1 - Practice # 6

Written Policies, Plans, Analysis

- Undocumented practices will no longer suffice because OCR would require documentation of all Security Rule policies, procedures, plans, and analyses.

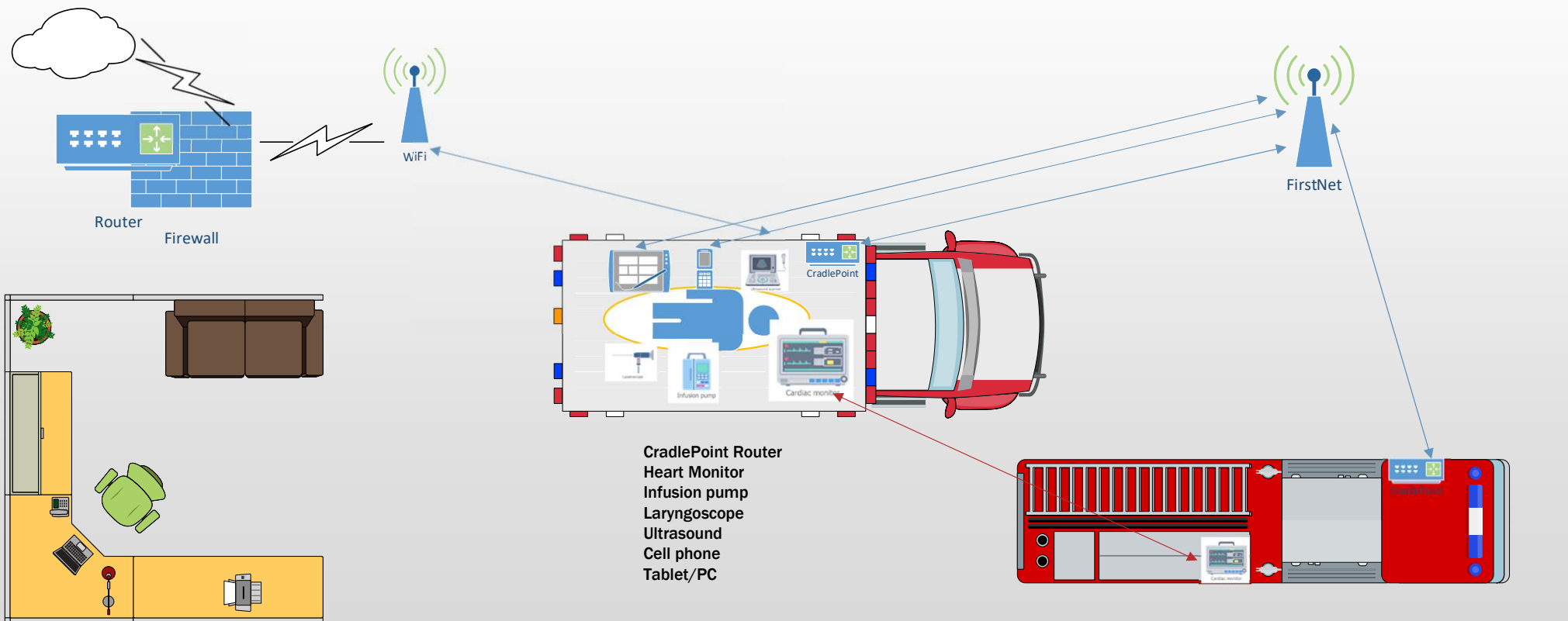


Network Maps & Asset Inventory

- Covered organizations would be required to have (and update every 12 months) a technology asset inventory and a network map illustrating the movement of ePHI throughout the regulated entity's electronic information system(s).



Notional Network diagram



Inventory your devices

- Include all cyber assets that “touch” ePHI
- Determine devices that include connectivity
- Identify devices that “retain” data

Cyber Asset inventory											Unit number: various
Communication											
Unit ID	Device	Manufacturer	Version/Firmware	WiFi	FirstNet	Bluetooth	NFC	Ethernet	USB	Other	Notes
Medic 3	WAN Comms	CradlePoint	Various	x	x						
Medic 3	Airpack comms	MSA				x	x				FD
Medic 3	Laptop (clinical)	GTA or Dell	Win 10 Pro	x		x					
Medic 3	Infusion pump	Sapphire	.7232, 1500 15.0.0						x		Eitan Medical (website) for updates
Medic 3	Verathon	Glidescope							x		Video
Medic 3	Lucas	Stryker		x		x					
Medic 3	Pulsara	iPhone		x	x						
Medic 3	Tablet	Samsung	Android	x		x					
Medic 3	Lumify Ultrasound	Phillips							x		Android
Medic 3	Tempus Heart Pro	Phillips	7.34	x	x			x			
Medic 3	Tempus Heart LS	Phillips	V1.3.5 10897	x	x	x					
Medic 3	CAD	Dell									
Workstation	QI/QC workstation	Dell	Win 10 Pro	x		x		x	x	Ext Drive	

Risk Analysis Assessment

- Previously, OCR did not offer a mandatory “checklist” for conducting a Risk Analysis. New express requirements would include a written assessment that contains, among other things:
 - A review of the technology asset inventory and network map.
 - Identify all reasonably anticipated threats to the confidentiality, integrity, and availability of electronic PHI (ePHI).
 - Identification of potential vulnerabilities and predisposing conditions to the regulated entity’s relevant electronic information systems
 - An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.



Contingency Planning and Security Incidents

- OCR would strengthen requirements for planning for contingencies and responding to security incidents and require organizations to:
 - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
 - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
 - Establish written security incident response plans and procedures that document how workforce members are to report suspected or known security incidents and how the regulated entity will respond to them.
 - Implement written procedures for testing and revising written security incident response plans.



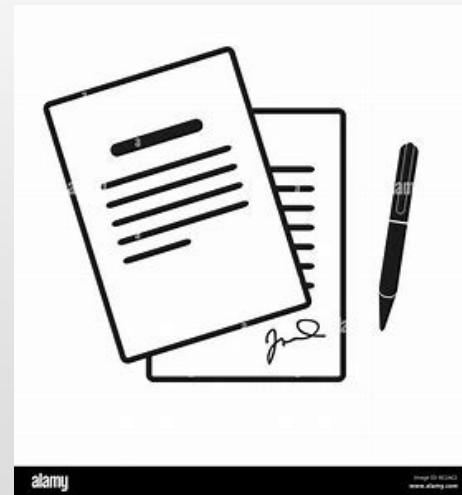
Annual Security Rule Audits

- OCR would require regulated entities to conduct a Security Rule audit at least once every 12 months.



Business Associate Verification

- The Proposed Rule would require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Business associates would also be required to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay but no later than 24 hours after activation.



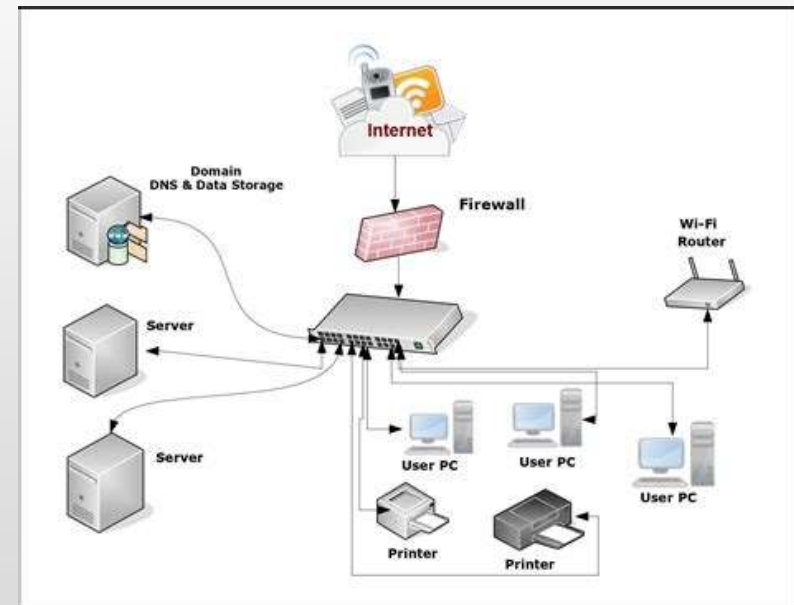
Encryption Requirement

- OCR would require encryption of ePHI at rest and in transit, with limited exceptions.



Required Technical Controls and Safeguards

- OCR wants to require regulated entities to have security measures, including:
 - Deploying anti-malware protection.
 - Removing extraneous software from relevant electronic information systems.
 - Disabling network ports in accordance with the regulated entity's risk analysis.
 - Network segmentation.
 - Separate technical controls for backup and recovery of ePHI and relevant electronic information systems



Multi-Factor Authentication

- OCR proposes to require the use of multi-factor authentication, with limited exceptions.



Vulnerability Scans and Penetration Testing

- Covered organizations would be required to conduct vulnerability scanning at least every six months and penetration testing at least once every 12 months.



**How this could affect
EMTs/Paramedics?**

What this means for EMS providers

- The HIPAA Security Rule is designed to safeguard electronic protected health information (ePHI) and ensure its confidentiality, integrity, and availability. If strengthened to address modern cybersecurity threats, the effects on EMTs and paramedics would primarily focus on compliance measures and operational changes involving how ePHI is handled, documented, and transmitted.

Increased Emphasis on Mobile Device Security

EMTs and paramedics often use mobile devices (e.g., tablets, smartphones, laptops) to document patient care and transmit ePHI to hospitals or dispatch systems.

Strengthened requirements may mandate:

- Encryption of ePHI stored or transmitted on these devices.
- Use of secure communication platforms to transmit patient data
- Enhanced device management protocols, such as remote wipe capabilities for lost or stolen devices.

Stricter Access Controls

EMTs and paramedics may face tighter rules for accessing ePHI, including:

- Use of multi-factor authentication (MFA) for logging into electronic systems.
- Role-based access to ensure only authorized personnel can view specific patient data.
- More frequent updates to credentials to reduce unauthorized access risks.

Mandatory Cybersecurity Awareness Training

EMTs and paramedics will likely be required to undergo enhanced cybersecurity training to:

- Recognize phishing and ransomware threats that could compromise ePHI.
- Understand secure methods for handling, storing, and sharing patient data.
- Learn about best practices for password management and device security.

Enhanced Incident Reporting

- EMTs and paramedics might need to follow stricter protocols for reporting suspected breaches or unauthorized access to ePHI.
- This could include documenting incidents immediately, reporting them to supervisors, and participating in investigations.

Audit and Monitoring of ePHI Access

- Strengthened rules may require healthcare organizations to audit EMT and paramedic access to ePHI regularly.
- This could result in additional administrative tasks, such as verifying proper use of systems and documenting compliance efforts.

Upgrades to Onboard Technology and Systems

Ambulance systems and equipment used by EMTs and paramedics (e.g., onboard computers, patient monitoring devices) may need:

- Software updates to comply with stronger encryption and cybersecurity standards.
- Replacement of outdated hardware that cannot meet the new requirements.
- Secure network connections for transmitting data to hospitals.

Potential Challenges in Remote and Emergency Settings

EMTs and paramedics often work in unpredictable and resource-limited environments.

Strengthened cybersecurity measures could create operational challenges, such as:

- Ensuring access to secure networks or devices in remote locations.
- Balancing patient care needs with the time required to follow security protocols.

Penalties for Non-Compliance

- If EMTs or paramedics fail to adhere to updated security rules, it could lead to disciplinary actions, fines for their organization, or legal liability.
- Ensuring compliance might require more oversight and accountability for daily practices.

More work and more cost

- Strengthening the HIPAA Security Rule will increase the responsibility of EMTs and paramedics to handle ePHI securely while introducing changes to technology, training, and daily workflows. These measures aim to protect patient data against modern cybersecurity threats *but may require additional resources and training to avoid disrupting emergency care services. Organizations employing EMTs and paramedics will need to prioritize these changes to ensure compliance and maintain operational efficiency.*

The Threat Landscape

- It's not a question of "If", it's a question of "When" there will be an incident.
- Daily, increasing threats to critical infrastructure.
- Awareness of the threats and taking proactive action when possible.

Cyber Intelligence Sources



Emergency Management & Response
Information Sharing & Analysis Center (EMR-ISAC)



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®



PSTA
Public Safety Threat Alliance
Public Safety ISAO



SAFE-D
Texas State Association of Fire and Emergency Districts

Protecting Critical Infrastructure Information from FOIA



What can we do?

50,000 foot view

- Monitor implementation of new/modified rules
- Start collecting information about your cyber assets (spreadsheet)
- Determine if you have the resources to achieve compliance with new rules
- Consider including preliminary cost in next budget

Where is the data and how are you protecting it?

- Cloud
- Medical device storage
- Temporary files on devices

ALS Medical Devices

- Increasing implementation of cyber components within our domain
 - Expect increase in capabilities/functionally, and more sophisticated software.
 - Will require patching
 - Supply chain considerations

Applications

- New software will be introduced that will require additional management
- Current software will increase in functionality and complexity
 - ImageTrend
 - Pulsara
 - Connectivity of handheld devices

Types of devices storing data

- Heart monitors
- Infusion pumps
- Larynscope
- Ultrasound



Where is data being stored?

- Cloud
- ImageTrend
- Pulsara
- Local workstations, external drives/USB's
- Cell phones/tablets
- Is it encrypted?



HIPAA Cybersecurity Compliance Assessment

Description	Y/N	Internal	External	Cost	Recurring	Comments
Required specifications applicable?						
Written Policies, Plans, Analysis?						
Network Maps & Asset Inventory?						
Risk Analysis Assessment?						
Contingency Planning and Security Incidents?						
Annual Security Rule Audits?						
Business Associate Verification?						
Encryption Requirement?						
Required Technical Controls and Safeguards?						
Multi-Factor Authentication?						
Vulnerability Scans and Penetration Testing ?						

Total \$0.00 \$0.00

Questions you should be asking

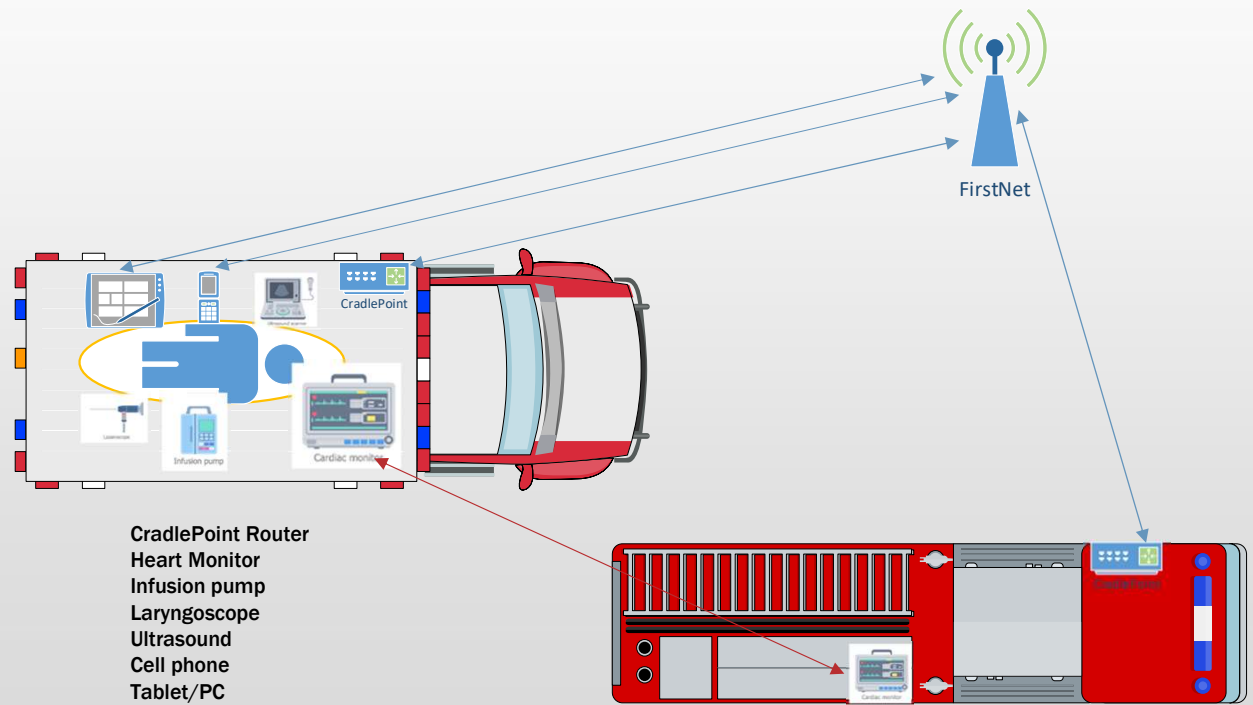
- What personnel have access to HIPAA information?
- How do they access the information?
- Can they save the information to a local device?
- Do you have procedures to delete data on a regular basis?

Questions

Contact Information

- Bob Janusaitis – bjanusai@business911.com
- Cell: 832-303-2911

Notional Network diagram



Please describe the topic you'd like to present	<p>This presentation will explore the rapidly evolving landscape of cybersecurity of in-field medical devices, emphasizing the growing vulnerabilities and advanced protection strategies that manufacturers and healthcare providers must adopt.</p> <p>With in-field medical devices becoming more interconnected and reliant on digital technologies, they are increasingly vulnerable to cyberattacks, raising concerns over patient safety, data security, and operational continuity.</p> <p>Key discussion areas include increase connectivity and cyber risks, vulnerability and exploitation in legacy devices, regulatory and compliance changes, emergence of artificial intelligence (AI), supply chain risks, and emerging protection standards.</p>
How do you feel this topic will be relevant to the SAFE-D audience?	<p>The presentation will provide:</p> <ul style="list-style-type: none"> • A general understanding of the current and future cyber threats facing medical devices. • Insight into regulatory frameworks and compliance requirements for securing medical devices. • Knowledge of the latest technologies and strategies being developed to combat cyber risks. • Practical steps for EMS providers to protect their medical devices from cyber threats. <p>The presentation aims to educate EMS professionals and cybersecurity experts on the evolving threats in in-field medical devices and the critical need for robust defense mechanisms.</p>

