

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

**AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA**

Secure Interoperability Products: Protecting Those Who Serve

Chris Wallace, Chief Cybersecurity, Program Executive Office, Defense Healthcare Management System (PEO DHMS)

Crystal Baum, Data Integration Solutions Director, Federal Electronic Health Record Modernization (FEHRM) Office

Antonnete Namai, Cybersecurity Director, FEHRM

Shawn Brody, Information Systems Security Manager (ISSM), Enterprise Intelligence and Data Solutions (EIDS)

Christopher Inman, Information Systems Security Engineer (ISSE), Joint Operational Medicine Information Systems (JOMIS)



Agenda

- 1** JOMIS Data Protections Process
- 2** EIDS Data Protections Process
- 3** Joint Health Information Exchange (HIE)
- 4** Trusted Exchange Framework and Common Agreement (TEFCA)
- 5** TEFCA Security and Operations

Speaker Introduction



**Chris Wallace,
Chief
Cybersecurity**

PEO DHMS



**Crystal Baum,
Data Integration
Solutions
Director**

FEHRM



**Antonnete Namai,
Cybersecurity
Director**

FEHRM



**Shawn Brody,
ISSM**

EIDS



**Christopher
Inman,
ISSE**

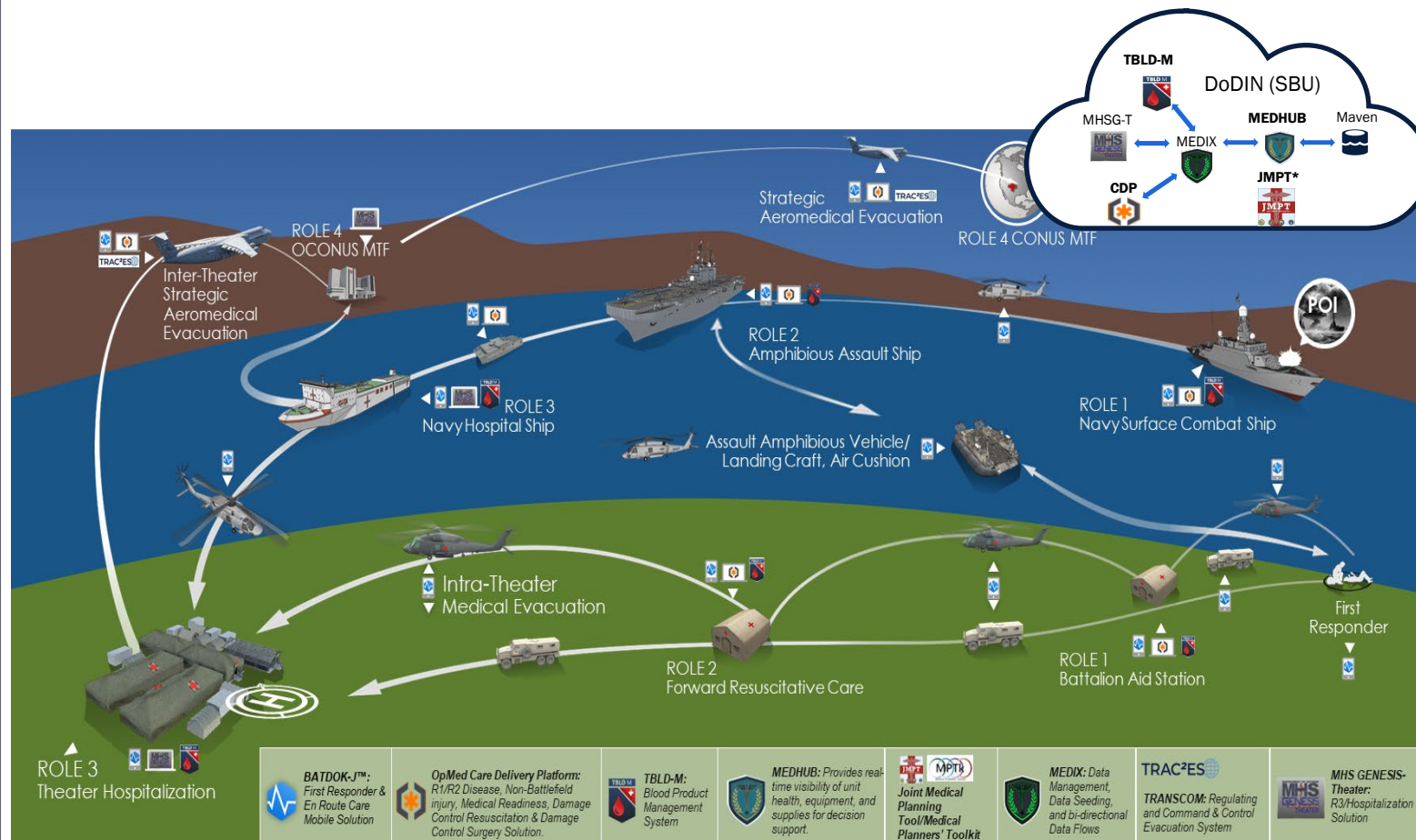
JOMIS

Learning Objectives

- 1** Present information that will allow the audience to formulate a better understanding of the efforts taken to secure the medical data from point of injury to the data repository.
- 2** Create an understanding of the requirements for securing the medical data and the effort to install trust and patient confidence that their data is maintained and available in a secure way.
- 3** Describe the Federal Electronic Health Record (EHR) interoperability solutions that allow secure access to critical data.
- 4** Explain the challenges associated with data integration ranging from legal, agency specific interests, etc.
- 5** Demonstrate how the Federal EHR ensures secure data interoperability.

Supporting the Warfighter with Modernized Healthcare Solutions

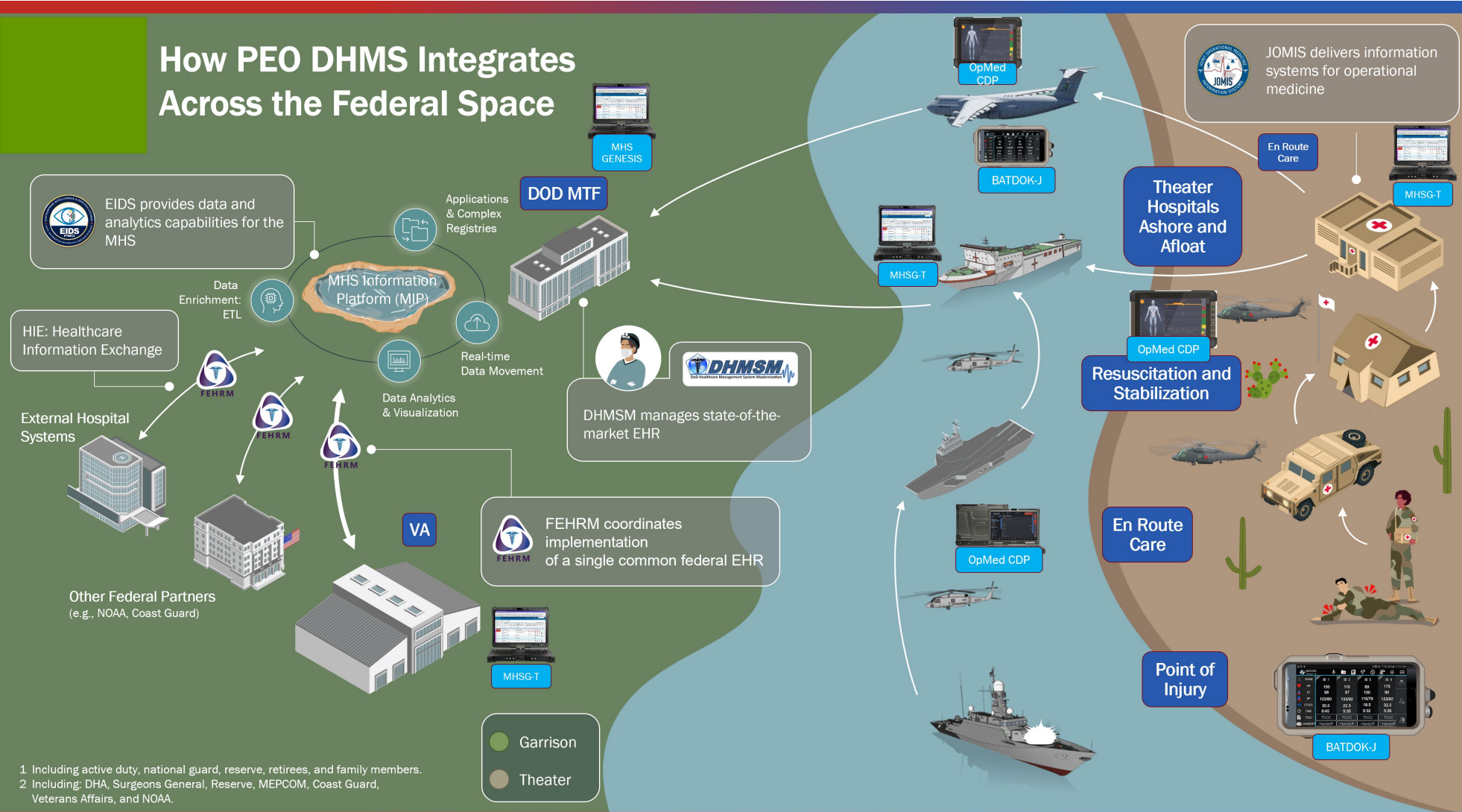
Enhancing Medical Readiness Against Evolving Threats



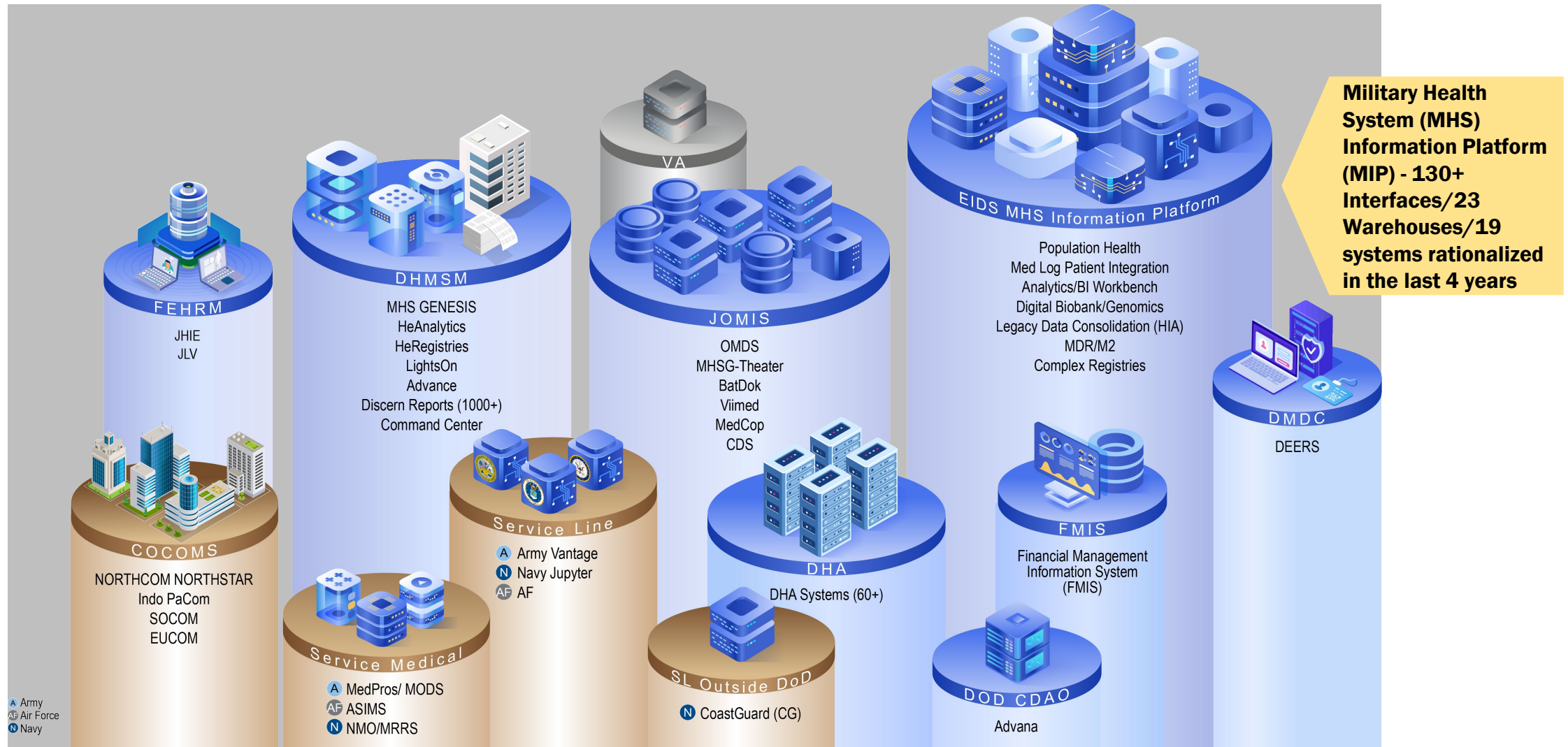
JOMIS Priorities

- 1 See the Battlefield**
 Deliver an integrated product suite of JOMIS capabilities (Healthcare Delivery, Theater Blood Mobile, MedHub), integrated together with Maven Smart System.
- 2 Trust the Data**
 Full medical C2/SA from the tactical level up to the Maven Smart system.
- 3 Predict**
 Cloud migration and model modernization for Joint Medical Planning Tool/Medical Planners' Toolkit.

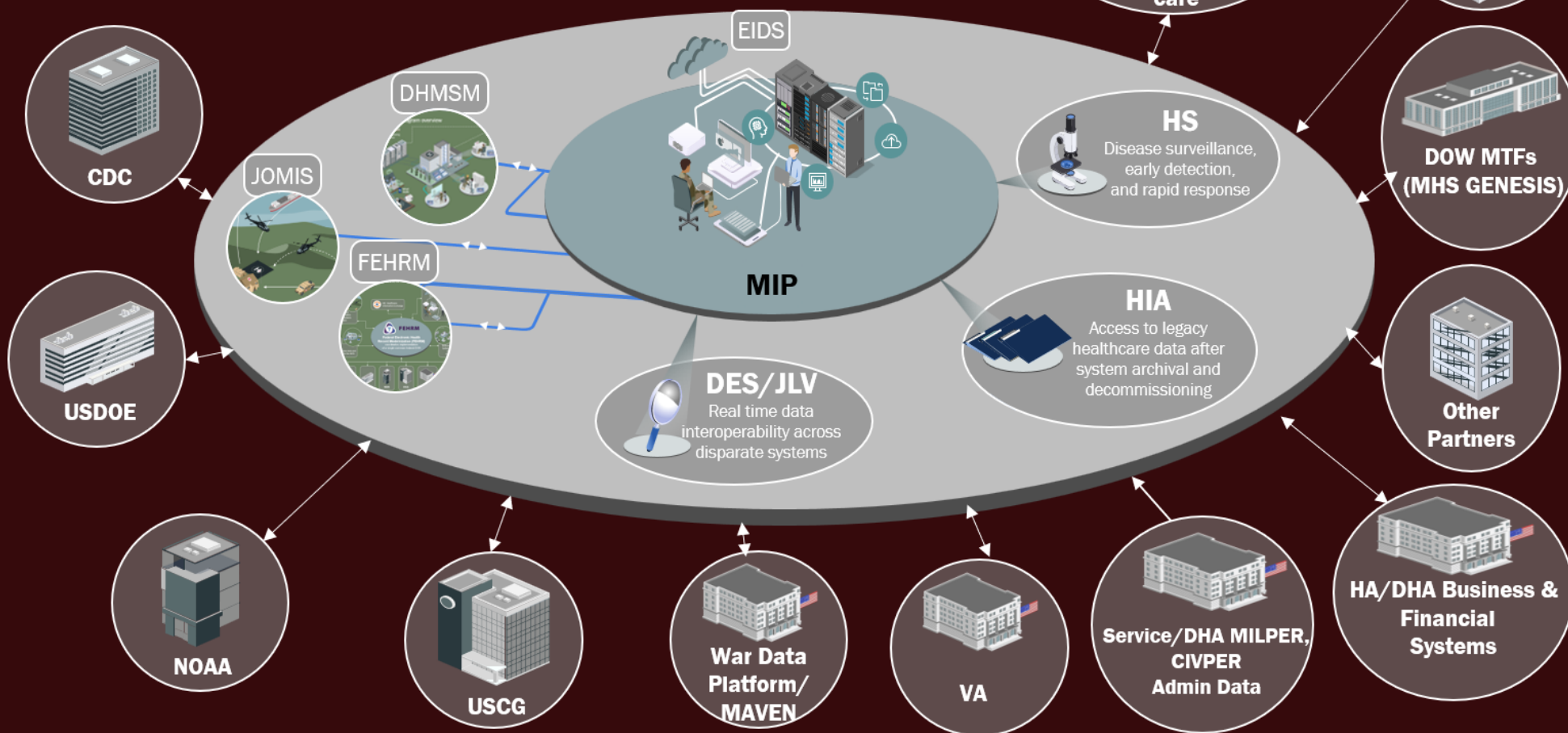
Federal Integration Capabilities



Complexity of Current Data Ecosystem



Military Health System Information Platform



EIDS delivers, connects, integrates, and curates health data to enable informed decisions, research, and innovation



MHS Information Platform

Provides a comprehensive analytics solution with flexible tools
Compiles aggregated data from 130+ DOW data sources on a scalable platform

MHS' Analytics and Data Visualization Platform



Digital Exchange Service

Joint Longitudinal Viewer

Pulls information from disparate health care systems in real time
Allows authorized users throughout DOW and VA to view clinical information



Health Information Archive

Enables the archival and decommission of DHA legacy systems
Provides clinicians with direct access to a patient's historical medical record



Health Surveillance

Collects near real-time data from MHS medical facilities to support the early detection and monitoring of health events
Provides prompt notifications of actionable and emerging health concerns

Outcomes/Achievements since EIDS standup in 2018

Maintains **LARGEST** repository of secondary data in DOW through rationalization of
30+ data warehouses

130+ data sources

Over 5.0 PB of active data

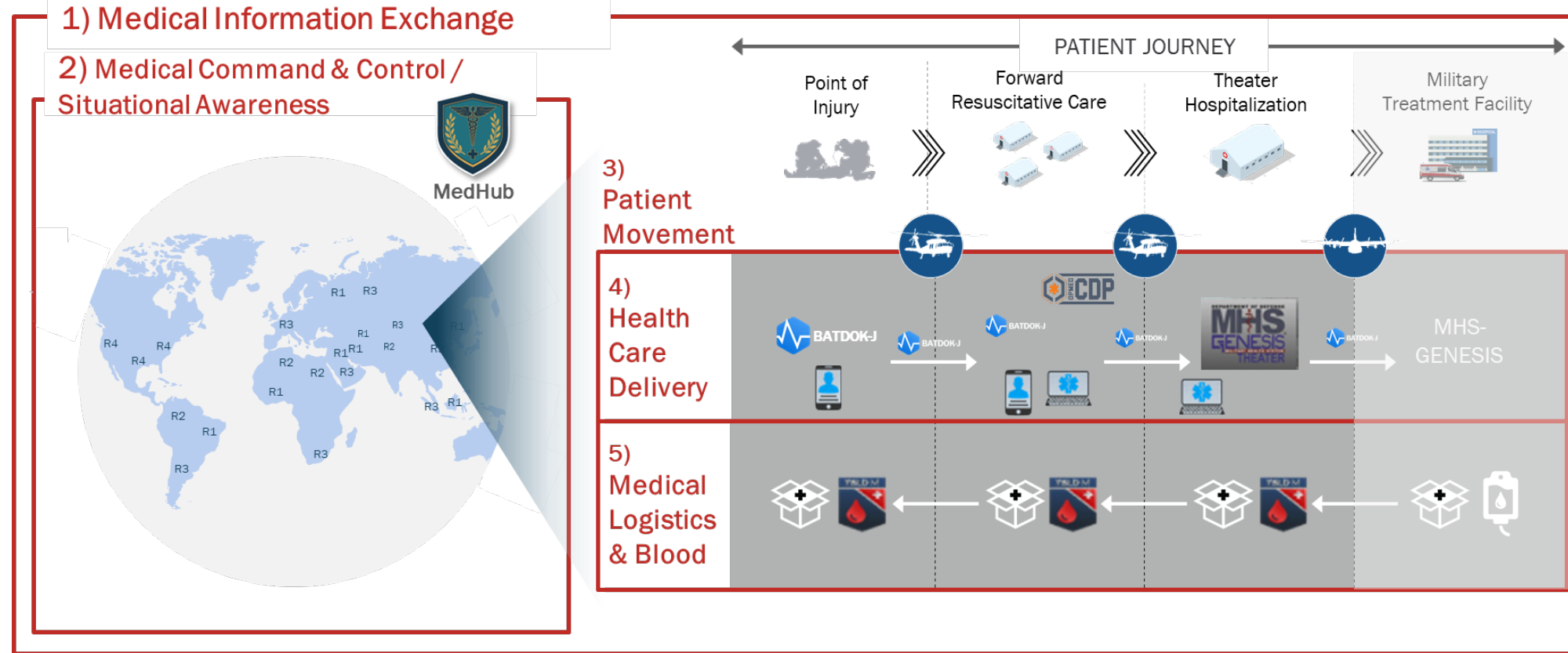
Rationalized & Developed 32 Applications

Conducted the **LARGEST DATA MIGRATION** in DHA's history, transferring over **60,000,000** health records annually

Modernized the Reserve Health Readiness Program (RHRP) for
800,000+ Remote component Service members and DOW Civilians

JOMIS's Portfolio: To Enable Comprehensive Health Care to Deployed Forces Across Full Range of Military Operations

JOMIS suite of solutions will drive **medical planning** for the warfighter with precision **health data** and advanced **health intelligence**.



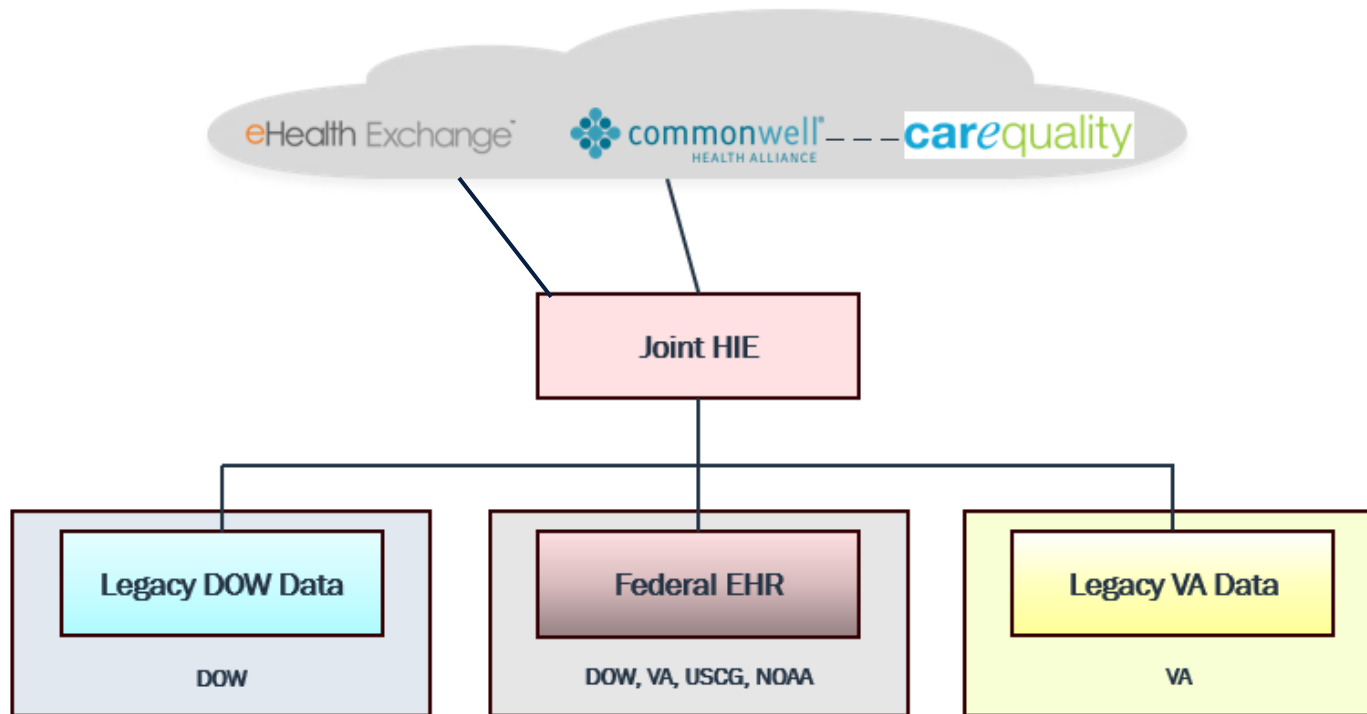
Note: BATDOK-J = Battlefield Assisted Trauma Distributed Observation Kit-Joint; CDP = Care Delivery Platform

Service Member's Longitudinal Health Record

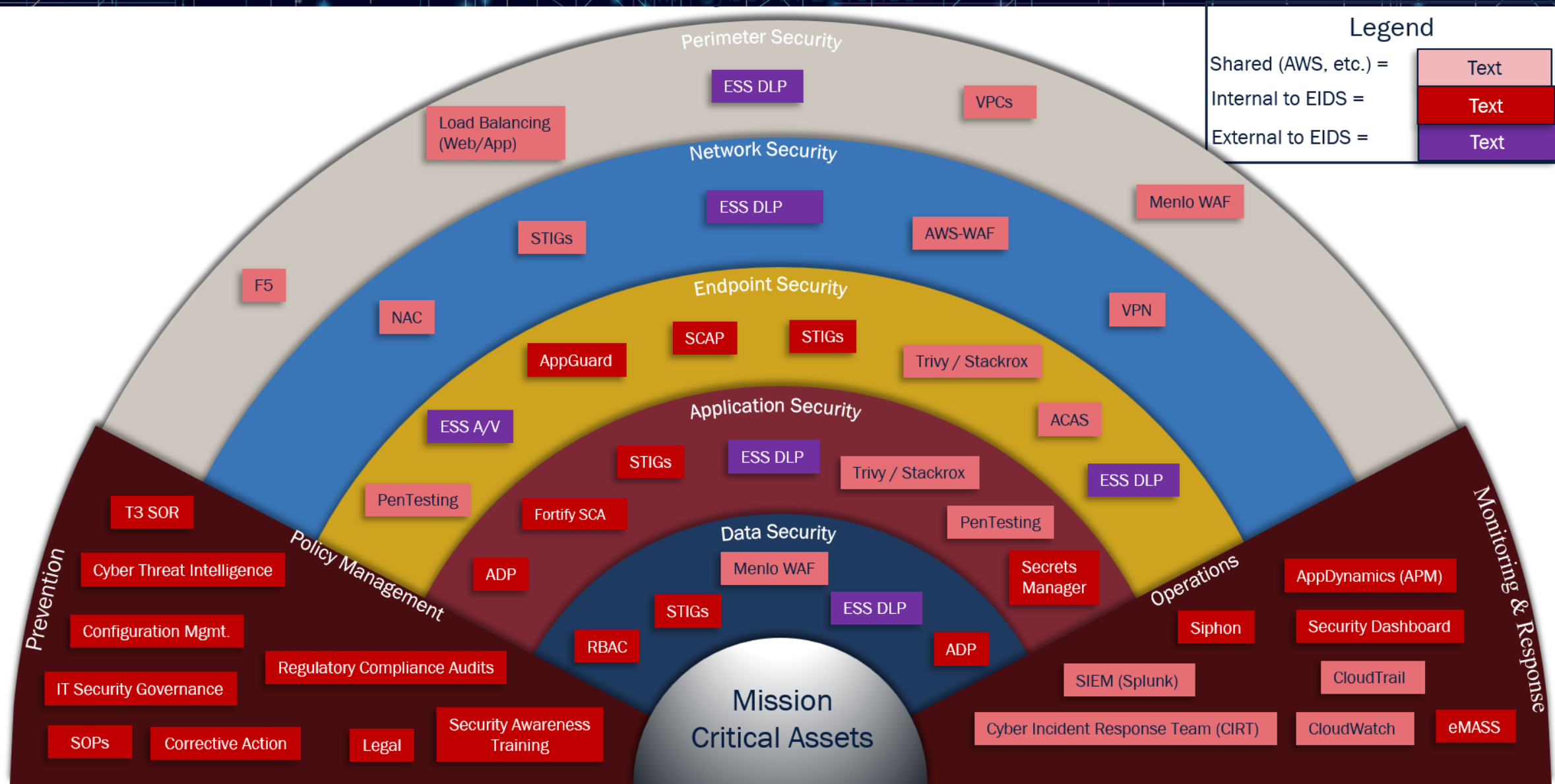
Protocols We Use to Secure the Path

- mTLS (mutual Transport Layer Security): Also known as Certificate Based Mutual Authentication (CBMA): This allows us to authenticate both the client and server.
- TLS 1.2 or TLS 1.3: Required by FIPS 140-2 and/or FIPS 140-3 to ensure data is protected while in transit.
- Apache Guacamole (HTTPS): Administrative access to our AWS environment is strictly controlled and managed via Apache Guacamole.

Joint Health Information Exchange (HIE)



- Joint HIE is connected to three major networks/frameworks allowing joint HIE access to over 90% of the U.S. hospitals and other organizations exchanging patient health data
- Enables **bi-directional exchange** of data with private sector
- Private sector partners receive consolidated federal data from the joint HIE acting as a single joint responder
- Federal partners are currently analyzing the best mechanism and timeframe to join the Trusted Exchange Framework and Common Agreement (TEFCA) in ~2026



UNCLASSIFIED

UNCLASSIFIED

Trusted Exchange Framework and Common Agreement

- TEFCA, established by the **21st Century Cures Act**, outlines a common set of principles, terms, and conditions for nationwide exchange of electronic health data.
- **Qualified Health Information Networks (QHINs)** are the central connection points within the network based on the Common Agreement, responsible for routing queries, responses, and messages among participating entities.
- TEFCA Exchange Purposes - Treatment, Payment, Healthcare Operations, Public Health, Government Benefits Determination, and Individual Access Services (IAS). *Only Treatment and IAS require responses from participants.*
- TEFCA is in a dynamic and developmental phase. Specifics are continually being refined through standard operating procedures (SOPs) and QHIN Technical Framework (QTF). Changes are being released quarterly. Recognized Coordinating Entity (RCEs) are still requesting clarification of what constitutes Treatment.

TEFCA Participation and the Federal EHR



Streamlines Access

- Brings HIEs under a single framework
- Eliminates need for multiple contracts, agreements, and connections
- Decreases costs



Standardization

- Common Agreement
- Standard Operating Procedures
- Technical Documents
- Single Governance structure under the RCE



Exchange Purposes

- **Approved Exchange Purposes:** Treatment, Individual Access Services, Health Care Operations, Payment, Public Health, Government Benefits Determination



Enhanced Security

- HiTrust compliance required for all QHINs
- Privacy and Security SOPs

Key Cyber Concerns and Considerations

- Expanded Attack Surface
- Data Security and Integrity
- Identity and Access Management
- Zero Trust and Network Security
- Application Programming Interfaces Security and Third-Party Risks
- Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the 21st Century Cures Act
- Threat Intelligence and Incident Response

TEFCA Security and Operations: Current Versus Future State

Inconsistent Security Practices

- Limited use of encryption; outdated or missing standards
- Weak access controls, often relying on basic username/password
- Reactive and fragmented incident management



Robust Security Framework

- Mandatory encryption protecting data at rest and in transit
- Access controls including multi-factor authentication and role-based access control enforcing strict access
- Incident management with proactive monitoring and breach-reporting timelines; outdated or missing standards

Fragmented Interoperability

- Data silos due to proprietary protocols and ad hoc agreements
- Inconsistent endpoint security across systems



Unified Interoperability Standards

- Seamless, secure data exchange across federal and non-federal entities
- Centralized governance via the RCE

Limited Compliance and Accountability

- Partial alignment with HIPAA; weak adoption of federal standards
- Inconsistent audit logs, leading to gaps in transparency
- Reactive and fragmented incident management



Compliance and Accountability

- Full alignment with HIPAA, Federal Information Security Management Act, and National Institute of Standards and Technology (NIST) Special Publication 800-53
- Comprehensive audit trails ensuring traceability

Patient and Operational Challenges

- Higher breach risks, undermining patient trust
- Inconsistent audit logs, leading to gaps in transparency
- Inefficiencies in data sharing, slowing care coordination



Improvements to Patients and Operations

- Reduced risks with stronger protections that restore trust
- Efficiency gains with streamlined data exchange that improves care delivery

Conclusion

The FEHRM's Cybersecurity Role in Analyzing TEFCA/QHIN Security Requirements:

- Participate in the TEFCA Cybersecurity Council to stay abreast of changes.
- Understand the Common Agreement and TEFCA Security and Trust Requirements to evaluate if the security controls outlined in the Assistant Secretary for Technology Policy's published security operating procedures meet DOW/VA Cybersecurity Requirements.
- Analyze the TEFCA third-party certification and cybersecurity framework to understand how it strengthens existing networks/frameworks and prevent incidents.
- Assess the impact of sharing Federal EHR data to ensure compliance, security, and patient privacy while evaluating risks and benefits to interoperability and data protection.
- Ensure proactive incident detection response and recovery strategies, including participation in cyber threat information-sharing networks, (i.e., U.S. Cyber Command, Cybersecurity and Infrastructure Security Agency, and industry stakeholders).
- Adopt zero trust architecture and security models, encryption and identity access management frameworks.

Contact

Chris Wallace

Chief, Cybersecurity

 christopher.c.wallace.civ@health.mil

Shawn Brody

ISSM, EIDS

 shawn.p.brody.civ@health.mil

Crystal Baum

Data Integrations Solutions Director

 crystal.a.baum.civ@health.mil

Christopher Inman

ISSE, JOMIS

 christopher.s.inman3.civ@health.mil

Antonnete Namai

Cyber Security Director

 antonnete.m.namai.civ@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Thank You!



UNCLASSIFIED