

Indian Health Service

Think Beyond Compliance

Strategic Approach to Securing Patient Data in Healthcare Networks

SOLOMON WILSON - IHS HQ

PROJECT MANAGER

AUGUST 24, 2023



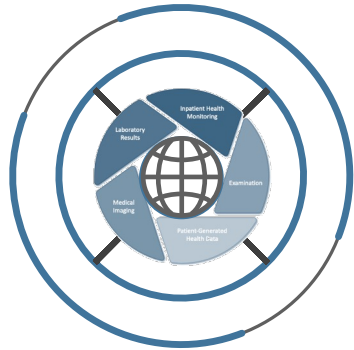
Think Beyond Compliance

Strategic Approach to Securing Patient Data in Healthcare Networks

Introduction



Key Highlights



Importance of patient data security in healthcare networks

Patient data security has become an ever-more critical priority for healthcare organizations in today's technologically sophisticated environment.

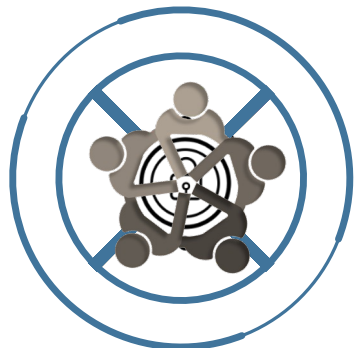
Data Elements:

Patient Family health history, lab/Imaging results, Rx, examination reports, financial information,



Collaboration among stakeholders to safeguard patient data

Healthcare organizations can collaborate with cybersecurity experts to stay updated on emerging threats and implement effective countermeasures.



Need for proactive measures beyond regulatory compliance

Security audits and vulnerability assessments can also help identify and address potential weaknesses in the system.



Risk of using Artificial Intelligence in the healthcare

AI brings with it concerns about data privacy and security. Ensuring that patient data is protected from bad actors is crucial in maintaining trust and confidence in the healthcare system.





Limitations of Relying on Regulatory Compliance

Many organizations rely solely on regulatory compliance for cybersecurity, but it has limitations and may leave them vulnerable to sophisticated cyber threats.

- 1 Minimum Standards
- 2 Reactive Approach
- 3 False Sense of Security

The Gap Between Compliance and Comprehensive Security

The gap between compliance and comprehensive security includes:

- 1 Inadequate Coverage
- 2 Lack of Flexibility
- 3 Emphasis on Checklists

Advancing Cybersecurity existing framework to follow a Proactive and Risk-Based Cybersecurity Approach

The Limitations of Reactive Cybersecurity:

- Delayed Detection and Response
- Incomplete Protection
- Increased Damage and Recovery Costs

The Benefits of a Pro-Active and Risk-Based Cybersecurity Approach in Healthcare:

- Early Threat Detection
- Optimal Resource Allocation
- Enhanced Incident Response
- Stakeholder Trust



THREAT LANDSCAPE IN HEALTHCARE

The evolving cybersecurity threats that target healthcare networks



Ransomware Attacks: Encrypts files and demands payment, making healthcare systems inaccessible.

Phishing and Social Engineering: Tricks employees into providing sensitive data or access to networks.

IoT Vulnerabilities: Exploits vulnerabilities in IoT devices to gain entry to networks or access patient data.

Insider Threats: Authorized employees pose a threat through negligence, malicious intent, or compromised credentials.

Data Leakage: Breaches healthcare networks to steal patient data for financial gain or identity theft.

Recent Real-World Examples of Healthcare Data Breaches:

1. SingHealth Data Breach-2018:

Personal information of **1.5 million** patients stolen.

2. Anthem Inc. Data Breach-2015:

Personal information of nearly **78 million** individuals exposed.

3. WannaCry Ransomware Attack-2017:

UK's National Health Service affected, causing delays in patient care.

4. LabCorp Data Breach-2019:

Personal and financial details of approximately **7.7 million** customers compromised.

5. Community Health Systems Data Breaches-2014:

Personal information of **4.5 million** patients compromised.

<https://meritalk.com/articles/cms-responds-to-data-breach-affecting-over-600000-medicare-beneficiaries/>

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (List of breaches in 2023)

Average ~\$429./ per incident total of ~\$500,000,000.00 +/- cost of the smallest breach listed on this slide

This is more than the ten year of IHS Security Budget

<https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far>

<https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector>





Secure patient data through a comprehensive, proactive plan aligned with organizational goals.

Educate employees on cybersecurity best practices to create a security-awareness in the environment.



Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

THE IHS – DIS STRATEGIC APPROACH

Implementing continuous monitoring by regular risk assessments to identification of potential vulnerabilities and assess threats and placing best prevention.

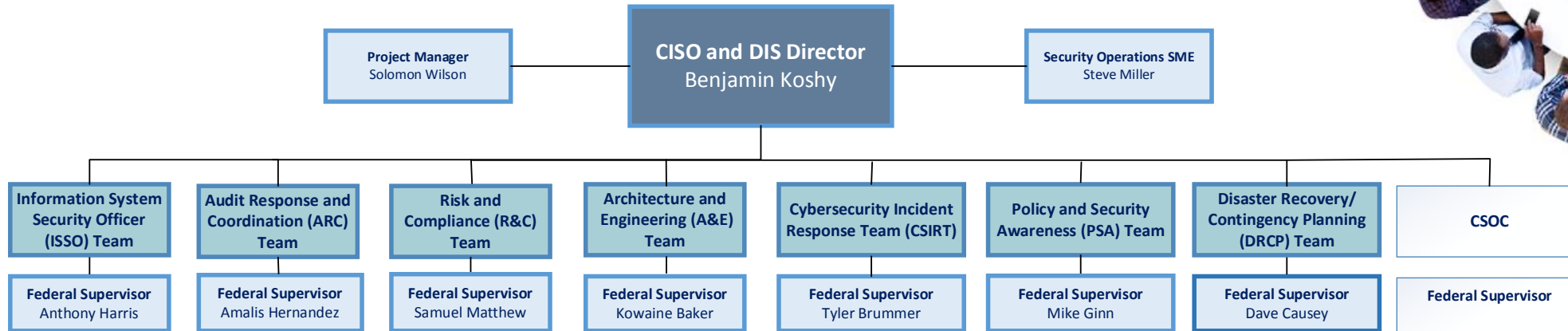


Modernizing IHS Cybersecurity Posture by implementing Agile processes



DIS consist of eight distinct cybersecurity functional areas to address the breadth of IHS cybersecurity needs while ensuring the program operated as cohesive unit.

- Project Management and Modernization (PM)
- Security Operation SME
- Information System Security Officer's (ISSOs)
- Risk and Compliance (R&C)
- Audit Response Coordination (ARC)
- Architecture and Engineering (A&E)
- Cybersecurity Incident Response (CSIRT)
- Policy and Security Awareness (PSA)
- Disaster Recover/Contingency Planning (DRCP)



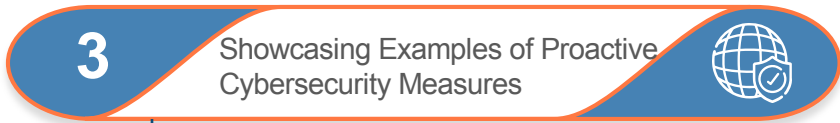
Healthcare industries store vast amounts of sensitive patient data, making them susceptible to cyber-attacks. While compliance is crucial, organizations must adopt proactive cybersecurity measures for better protection.



- **Comprehensive Security:** Going beyond compliance allows for a more thorough security strategy that addresses emerging threats.
- **Proactive Threat Mitigation:** Continuous monitoring helps mitigate risks before they escalate.
- **Faster Incident Response:** Proactive measures enable swift detection and response to cyber incidents.



- **Patient Privacy:** Breaches erode patient trust in healthcare systems.
- **Legal Compliance:** Violations lead to regulatory fines and legal consequences.
- **Reputational Damage:** Breaches can harm an organization's reputation.



- **Mayo Clinic:** Invests in robust cybersecurity, employee training, and collaboration with experts.
- **Cleveland Clinic:** Implements multi-layered security, encryption, and a dedicated incident response team.
- **Kaiser Permanente:** Engages in continuous monitoring, threat intelligence sharing, and employee education.



DIS Comprehensive cybersecurity framework tailored for IHS

The healthcare faces unique challenges in cybersecurity due to the sensitive nature of patient data and require tailored comprehensive Cybersecurity Framework



1

Employee Training: Human error remains a significant cybersecurity threat in healthcare settings

Aligning Requirements with Security Objectives: Managing Identified Threat and Building Secure Solutions.

2

3

Threat Intelligence: Threat intelligence involves monitoring and analyzing information about cybersecurity threats and adversaries.

Incident Response: An incident response plan outlines the steps and procedures to be followed during a cybersecurity incident.

4

5

Security Controls: Security controls are measures and safeguards to protect against cybersecurity threats.

6

Risk Assessment: A risk assessment is the foundation of a cybersecurity framework for healthcare organizations.

Building Safer Secure Future with Collaboration: build effective security solutions, and fortify our infrastructure.

7

8

Resolve identified Weakness: implement effective weakness identifications resolution and reporting methods

Effective Business Continuity: Develop business impact analysis, Recovery time and Point Objectives, and test effectiveness of CPs

9

10

Continuous Strategic Alignment: Develop KPIs for all DIS services to validate the performance and enhance strategic objectives



EMPLOYEE TRAINING AND AWARENESS

Training of Employees is essential in protecting sensitive information.
Key points highlighting the importance of employees



Employee Training and Awareness

When it comes to maintaining data security. Our Employees who provide any type of services to deliver the IHS mission, are our front line defense. They are the first one who face the real threat, they are the crucial force, boots on the ground encountering and responding to real time threats while delivering their services.

Access Control

Make them responsible to watch their actions for exercise their authorities while accessing the data they need for their jobs.

Adherence to Policies

The employees must adhere to all policies. It is essential to use strong passwords and update software and systems regularly.

Reporting Suspicious Activities

Encouraging employees to report any suspicious activities or security breaches immediately is essential.

Mobile Device Security

Since mobile devices have become an increasing part of workplace life, employees must understand how to secure them properly.

Physical Security

Employees must also consider physical security measures, such as locking up their workstations, shredding confidential documents, or using secure disposal methods.

Continuous Learning

Cybercriminals are constantly evolving, and employees need to stay updated about the latest trends and techniques they use.



Educating And Raising Awareness

Comprehensive Program of Training Awareness Highlights of Employee Training Program Strategy



Develop a comprehensive program of training

Create a training program with a structure that includes patient care, safety protocols, and ethical considerations

Use interactive and engaging methods

Incorporate interactive elements into your training sessions, such as role-playing, case studies, and group discussions.

Continued education opportunities

Provide opportunities for continuing education, such as webinars, workshops, seminars, and conferences.

Foster a culture that encourages learning

Create an environment where learning and development are encouraged.

Use technology-based tools

Use technology-based platforms and mobile applications like eLearning to provide educational content to healthcare professionals.

Involve experts from multiple fields

Work with experts in different departments or specialties to create specialized workshops.

Implement peer-to-peer learning

Encourage experienced healthcare professionals to mentor younger team members.

Implement peer-to-peer learning

Encourage experienced healthcare professionals to mentor younger team members.

Open communication channels

Encourage open communication between healthcare professionals and management

Include real-life examples

Use real-life cases or examples to illustrate certain healthcare practices or protocols' importance.

Recognize learning achievements and reward them

Reward and acknowledge healthcare staff that actively participates in educational programs.



Information System Security Officer

Evaluating Business Objectives, Aligning Security Objectives, Managing Identified Threat and Building Secure Solutions



Embrace Collaboration with the ISSO

Bring your requirements and requests to the ISSO, who will help guide you in meeting these crucial standards and ensuring the security of our systems.

Enhance Cybersecurity Journey with the ISSOs

Share your requirements and seek expert guidance to ensure that your systems adhere to the rigorous cybersecurity standards mandated by the federal government and industry regulations. Establish a secure environment that meets and exceeds these requirements.

Establish Trust with the ISSO

By involving the ISSO in your requirements and requests, you can navigate the complexities of federal government and industry cybersecurity standards

Elevate Cyber Defense with ISSO's Expertise

Through collaboration, the ISSO can provide critical insights and guidance to meet the cybersecurity requirements set by the federal government and industry standards. Let us partner together to safeguard our systems and protect against cyber threats.

Inspire a Culture of Cybersecurity Excellence

By bringing your requirements and requests, you contribute to our collective commitment to meeting federal government and industry cybersecurity standards. Together, we can foster a resilient security posture that protects our organization and upholds the highest levels of data and information security.

Empower Healthcare Modernization with ISSO

Unlock the potential of the DIS ISSO Group to drive healthcare modernization and fortify security. Leverage their expertise, resources, and guidance to navigate the complexities of evolving technologies. Together, we can transform healthcare, ensuring data protection, and enabling innovative advancements. Seek the DIS ISSO Group's support today and embark on a journey of secure and transformative healthcare solutions



INCIDENT RESPONSE AND PREVENTION

The significance of having a robust incident response plan in place



Unlock the Power of DIS CSIRT Resources

Tap into the invaluable Cyber Security Incident Response resources provided by (DIS). Utilize the resources to assist you conduct a thorough research, mitigate threats, recover from incidents, and implement preventative measures that align with stringent cybersecurity requirements set by the federal government and industry standards. Together, let's create a safer environment for delivering healthcare services

Empower Yourself with CSIRT Capabilities

Utilize the tools implemented by DIS CSIRT and A&E teams to conduct in-depth research on cybersecurity incidents, proactively mitigate vulnerabilities, and establish robust recovery strategies. By utilizing tested preventative methods, we can meet the cybersecurity requirements of the federal government and industry standards, ensuring a secure healthcare service delivery environment.

Establish Trust and Resilience with DIS

Identify and remove weaknesses, implementing preventative measures that comply with federal government and industry cybersecurity requirements. Together, we can create a secure environment where healthcare services can be delivered confidently.

Elevate Cybersecurity Excellence

Partnering in the effort to deliver services and protect the valuable information of our patients, we can exceed the cybersecurity requirements of the federal government and industry standards, resulting in a safer environment for delivering healthcare services.

Inspire a Culture of Cybersecurity Preparedness

Embrace DIS's Cyber Security Incident Response resources to inspire a culture of cybersecurity preparedness. Utilize these resources to identify weak spots, mitigate risks, and establish preventive measures that address federal government and industry cybersecurity requirements. Together, we can create an environment where healthcare services are delivered securely, protecting patient data and instilling confidence in our stakeholders.



Collaborative Security Architecture Engineering (A&E)



Security By Design

Engage with the DIS A&E Team

Bring your new requests to DIS A&E team so they can assist you evaluating the technology and make sure the solutions we acquire are safe to use, so you can make an informed recommendation and choose secure solutions that align with your requirements. Together we select the technology that are safe from potential threats.

Elevate Your Security

Share your requests and tap into DIS A&E expertise to gain a comprehensive security overview. Equip yourself with the knowledge to make informed decisions and select solutions that prioritize safety and protection.

Building a Secure Future Together

By involving DIS A&E in your advancement journey, you can ensure that every solution meets stringent security requirements. They can help you establishing a robust foundation that safeguards our systems for years to come.

Add Security In Your Priority

Engaging with the Security Architecture and Engineering Group shows your commitment to making security a top priority. Seek their guidance and integrate their insights in the evaluation of your new requests. By working together, we can create a culture of security where protection is at the forefront of decision making.

Unleash the Power of Collaboration

The Security Architecture and Engineering Group thrives on collaboration. Engage with A&E team and witness the collective power of our teams. By working hand in hand, we can overcome challenges, build effective security solutions, and fortify our infrastructure. Together, we can achieve greater resilience and peace of mind.

Building Safer Secure Future with Collaboration

Collaborating with the Security Architecture and Engineering Group is key to revolutionizing healthcare. Together, we can create a secure future where patient records are protected, medical devices are shielded, and telehealth platforms are trusted. By integrating strong security measures into healthcare technologies, we empower innovation and ensure excellence in patient care. Let's collaborate today to build a world-class healthcare system that prioritizes security and transforms lives



Robust Audit Coordination and POAM Management



Managing Identified Threat and Monitoring Resolution Efforts

Utilize POAM Mgt. and ARC Resources

Leverage the Division of Information Security's (DIS) POAM management resources to meet federal government and industry cybersecurity requirements. Use these valuable tools to identify, address, and remove weaknesses, ensuring compliance and fortifying our cyber defenses.

Ease Your Cybersecurity Journey with DIS-ARC

Engage with DIS's POAM management resources as a catalyst for your organization's cybersecurity journey. Embrace the opportunity to respond to data calls and address identified weaknesses promptly.

Inspire Proactive Cybersecurity Practices

By addressing weaknesses and enhancing our cybersecurity posture, we pave the way for a secure future that easily adheres to federal government and industry requirements.

Establish Trust Achieve Security Compliance

By utilizing DIS's POAM management resources, you demonstrate your commitment to trust and compliance. Effectively utilize these tools to respond diligently and in a timely fashion to data calls, rectifying any identified weaknesses. Through our collective effort, we can establish robust cybersecurity practices that exceed industry standards.

Elevate Cybersecurity Resilience

Maximize the potential of DIS's POAM management resources to elevate your organization's cybersecurity resilience. Use the knowledge and experience our DIS POAM team brings to strategically address weaknesses, implementing appropriate security measures in line with federal government and industry standards.

Collaboration with DIS PAOM and ARC

Embrace the opportunity to collaborate with DIS's PAOM and Audit Response Coordinator Team. By engaging with them, you can proactively address weaknesses, easily adhere cybersecurity practices, and ensure seamless compliance and continue monitoring with government and industry standards. Empower IHS Mission through this dynamic partnership, driving resilience and inspiring a secure future.



Comprehensive Risk Assessment Program



Holistic Risk Management Framework

Engage with the DIS Risk and Compliance Team

Building partnership with the Division of Information Security's (DIS) Risk and Compliance team results strengthening your system security and help implementing the controls that protect our systems from bad actors and insider threats. By utilizing R&C expertise, we can ensure that our systems are secure, and appropriate controls are in place weaknesses are addressed to deliver the services.

Empower Cybersecurity Strategy with DIS R&C

Leverage R&C resources to identified cybersecurity weaknesses to protect the data our patients, delivering the services in secure manner, enhancing the trust of our community and helping to achieve the goal of IHS Mission delivery.

Establish Trust and Proactive Security Measures

Building trust and enacting proactive security measures go hand-in-hand with DIS's Risk and Compliance team. Utilize their expertise to evaluate controls, identify potential vulnerabilities, and implement the right measures to address them.

Elevate Cybersecurity Resilience

Elevate your organization's cybersecurity resilience by collaborating with DIS's Risk and Compliance team. Utilize their knowledge and resources to assess controls, identify weaknesses, and implement robust security measures. By aligning with federal government and industry cybersecurity requirements, we lay a strong foundation for a secure healthcare service delivery environment.

Build a Culture to Assess Security first

Engage with them to assess controls, address weaknesses, and establish a proactive security posture. Together, we create an environment where healthcare services are delivered with confidence, ensuring the protection of sensitive data and mitigating potential risks from bad actors and insider threats.



Resilient Disaster Recovery and Contingency Plan



The importance of Business Continuity

Build Comprehensive BIAs and CPs

Foster collaboration with the Division of Information Security (DIS) to develop, implement, and test comprehensive Business Impact Analyses (BIAs) and Continuity Plans (CPs). By working together, we can identify critical functions, evaluate risks, develop effective plans, and ensure compliance with federal government and industry cybersecurity requirements. Let's create a resilient environment for delivering healthcare services.

Empower Your Business Continuity Strategy

Leveraging DIS DRCP team expertise help empowering IHS placing robust continuity strategy. Engage with DRCP team to develop comprehensive BIAs and CPs, implement them effectively, and rigorously test their effectiveness. Collaboration with DRCP team help establishing a secure and resilient environment for healthcare service delivery.

Develop, Implement, and Test CPs in Partnership

Partner closely with DIS to ensure the development, implementation, and testing of robust Continuity Plans (CPs). Utilize their guidance and resources to develop customized plans that align with federal government and industry cybersecurity requirements. Implement and rigorously test these plans to enhance resilience and response capabilities, thereby ensuring uninterrupted healthcare service delivery

Build Resilience through BIA and CP Development

Collaborate with DIS to conduct thorough assessments, develop tailored plans, and guide their effective implementation. Testing CPs regularly ensures their efficacy and enables us to meet federal government and industry cybersecurity requirements, safeguarding healthcare service delivery.

Test






Engage in the development, implementation, and rigorous testing of BIAs and CPs to demonstrate a proactive commitment to meeting federal government and industry cybersecurity requirements. With DIS's support, we can create a resilient environment where healthcare services thrive without interruption.

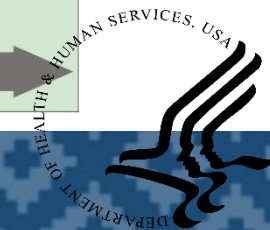


Future of IHS Cybersecurity

DIS Plan from FY24 – FY26



	Identity 	Device 	Network / Environment 	Application Workload 	Data 
Traditional	<ul style="list-style-type: none"> • Password or multifactor authentication (MFA) • Limited risk assessment 	<ul style="list-style-type: none"> • Limited visibility into compliance • Simple inventory 	<ul style="list-style-type: none"> • Large macro-segmentation • Minimal internal or external traffic encryption 	<ul style="list-style-type: none"> • Access based on local authorization • Minimal integration with workflow • Some cloud accessibility 	<ul style="list-style-type: none"> • Not well inventoried • Static control • Unencrypted
	<p>← Visibility and Analytics Automation and Orchestration Governance →</p>				
Advanced	<ul style="list-style-type: none"> • MFA • Some identity federation with cloud and on-premises systems 	<ul style="list-style-type: none"> • Compliance enforcement employed • Data access depends on device posture on first access 	<ul style="list-style-type: none"> • Defined by ingress/egress micro-perimeters • Basic analytics 	<ul style="list-style-type: none"> • Access based on centralized authentication • Basic integration into application workflow 	<ul style="list-style-type: none"> • Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	<p>← Visibility and Analytics Automation and Orchestration Governance →</p>				
Optimal	<ul style="list-style-type: none"> • Continuous validation • Real time machine learning analysis 	<ul style="list-style-type: none"> • Constant device security monitor and validation • Data access depends on real-time risk analytics 	<ul style="list-style-type: none"> • Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted 	<ul style="list-style-type: none"> • Access is authorized continuously • Strong integration into application workflow 	<ul style="list-style-type: none"> • Dynamic support • All data is encrypted
	<p>← Visibility and Analytics Automation and Orchestration Governance →</p>				



Questions Concerns





THE IMPORTANCE OF CONDUCTING COMPREHENSIVE RISK ASSESSMENTS



Importance of comprehensive risk assessments:

- Importance of comprehensive risk assessments:
- Identifying internal and external risks.
- Prioritizing risks based on impact and likelihood.
- Planning for risk mitigation.
- Supporting decision-making at all organizational levels.



Process of identifying, prioritizing, and mitigating risks:

- Identifying risks through data gathering and analysis.
- Assessing risks based on impact and likelihood.
- Prioritizing risks for resource allocation.
- Developing mitigation strategies.
- Monitoring and reviewing implemented strategies.

