

**2026 DEFENSE  
HEALTH INFORMATION  
TECHNOLOGY SYMPOSIUM**

August 11-13, 2026  
Hyatt Regency New Orleans  
New Orleans, LA

# Managing Shadow IT: Understanding the Why

*MAJ(P) Daniel H. Lister, MSN, BSN, BC  
Chief of Medical Management, Evans Army Community Hospital*

*MAJ(P) Adam O. Rich, MS, RN  
CHIO, Womack Army Medical Center*

*Ms. Yolanda J. Farmer  
CIO, Womack Army Medical Center*

*Mr. Kirby J. Lyford  
CIO, Landstuhl Regional Medical Center*

UNCLASSIFIED

UNCLASSIFIED



2026 DHITS 1

# Disclaimer

*“The views expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of the Defense Health Agency, Department of Defense, nor the U.S. Government.”*

# Agenda

- 1** Speaker Introductions
- 2** What is Shadow IT?
- 3** The Clinical End-User Perspective: Why They Use Shadow IT
- 4** Understanding the Why: IT Perspective and Risks
- 5** Real-World Examples
- 6** Strategies for Mitigation, The 80 Percent Solution, and Path to YES
- 7** Lifecycle, Engagement & Change Management
- 8** Call to Action / Q&A

# Speaker Introduction

## **MAJ(P) Daniel H. Lister, MSN, BSN, BC**

Chief of Medical Management, Evans Army Community Hospital

MAJ(P) Daniel H. Lister is the Chief of Medical Management for Evans Army Community Hospital and previously served as the Deputy Nursing Informatics Consultant to the Surgeon General. He served as CHIO for Carl R. Darnall Army Medical Center and interim CHIO for Defense Health Network West during the DHA market-to-network transition. MAJ Lister holds a Master's in Nursing Informatics from the University of Utah and is board-certified in nursing informatics.

---

## **MAJ(P) Adam O. Rich, MS, RN**

CHIO, Womack Army Medical Center

MAJ(P) Adam Rich is the CHIO for Womack Army Medical Center and Co-Chair for the DHN-E ISC. He previously served as an Informatics Officer for Brooke Army Medical Center and has 16 years of nursing experience. MAJ Rich holds a Master's in Biomedical Informatics from the University of Utah and brings unique expertise in identifying and managing Shadow IT within military health settings.

# Speaker Introduction (Cont'd)

## Ms. Yolanda J. Farmer

CIO, Womack Army Medical Center

Yolanda J. Farmer is the Chief Information Officer (CIO) for Womack Army Medical Center, Fort Bragg, NC. She previously served as Deputy CIO, Project Manager, Systems Analyst, and in various other key IT roles across both Army Medical Command (MEDCOM) and the Defense Health Agency (DHA), bringing over 20 years of hands-on healthcare IT experience to the panel. Ms. Farmer holds multiple elite industry credentials, including Security+ and PMP, and brings unique expertise in structured project management, business process optimization, and engineering efficient IT workflows across the military health enterprise.

---

## Mr. Kirby J. Lyford

CIO, Landstuhl Regional Medical Center

Mr. Kirby Lyford is the CIO at Landstuhl Regional Medical Center. He's spent the last 17+ years working across Army MEDCOM and DHA, helping shape how technology supports military healthcare. He has led large-scale efforts from DHA's first enterprise level deployment rollout (Win10) to other key programs with PEO D2D, including critical work with MedCOI migration. Before transitioning to Healthcare IT, he served 11 years as an Infantryman in the US Army. He is currently focused on improving how IT works at the MTF level by using automation and AI to streamline processes and support the people who care for our beneficiaries.

# Learning Objectives

- 1** Describe the challenges and risks associated with Shadow IT in healthcare IT environments, focusing on the why behind both user behavior and IT concerns.
- 2** Articulate the clinical end-user perspective and the genuine patient care drivers that lead clinicians to adopt Shadow IT solutions.
- 3** Explain how lifecycle management can address the root causes of Shadow IT while improving oversight and governance.
- 4** Apply change management techniques to align clinical needs with IT policies, ensuring successful adoption of approved technologies.
- 5** Evaluate the benefits of the 80 percent solution in addressing user needs while maintaining compliance and operational efficiency.

# What is Shadow IT?

Shadow IT refers to any information technology system, software, or service used within an organization **WITHOUT** explicit approval or oversight from the IT department.

- Common forms of Shadow IT include:
  - Personal devices used for work-related communication or documentation (not AVD or BYOD)
  - Third-party or consumer-grade applications not vetted for security or HIPAA compliance
  - Cloud services outside of approved enterprise platforms (e.g., personal Google Drive, Dropbox)
  - Unauthorized communication platforms such as Signal, WhatsApp, or personal email and text messages
  - Locally built databases or tracking tools (e.g., Access databases, Excel trackers with PHI)
  - Unapproved AI tools used for clinical decision support or documentation assistance
  - Remote access to clinical systems from unapproved locations or devices

# Shadow IT in Clinical World

*These are the voices we hear every day. Understanding them is the first step toward meaningful change.*

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICU Nurse          | "I texted the on-call physician because the approved system was down and I needed an urgent order. My patient could not wait."                                               |
| Physical Therapist | "We built a spreadsheet to track our patients because MHS GENESIS does not capture what we need for our workflow. It took years to build and everyone relies on it now."     |
| Deployed Medic     | "We used Signal to coordinate patient handoffs because we had no access to approved communication tools in the field. We were just trying to keep the patient alive."        |
| Pharmacy           | "We use Waitwhile application to improve customer flow."                                                                                                                     |
| Orthopedic Surgeon | "The AI tool we use for preoperative planning is far better than anything the system offers. We purchased it ourselves because waiting for approval would have taken years." |

# The Clinical End-User Perspective

## Why Clinical End-Users Turn to Shadow IT

|                                |                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Patient Care First:</b>     | The primary driver is always patient care. If an approved system is unavailable, too slow, or does not support the clinical workflow, clinicians <u>will</u> find another way.                                                                                 |
| <b>Workflow Gaps:</b>          | Approved tools often do not cover every clinical scenario. Gaps in functionality force clinicians to build workarounds using whatever tools are available.                                                                                                     |
| <b>Time Pressure:</b>          | In fast-paced clinical environments, speed matters. If a personal device or app is faster than the approved solution, clinicians will default to what works in the moment.                                                                                     |
| <b>Communication Barriers:</b> | Approved communication platforms may be difficult to access, require additional logins, or lack mobile capability - pushing clinicians toward utilizing personal third-party texting or email platforms (WhatsApp, iMessage, etc.) to coordinate patient care. |
| <b>Lack of Awareness:</b>      | Many clinicians are unaware that the tools they are using are classified as Shadow IT or that approved alternatives exist or are in development.                                                                                                               |
| <b>Cultural Normalization:</b> | When workarounds become standard practice within a team or unit, new staff adopt them without question, embedding Shadow IT into clinical culture.                                                                                                             |

# The Clinical End-User Perspective (Cont'd)

## Why Clinical End-Users Turn to Shadow IT

|                        |                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Efficiency of Workload | Clinicians will utilize Shadow AI by integrating unsanctioned consumer chatbots (like ChatGPT) and pasting Protected health Information (PHI) for the purpose of drafting emails and clinical notes                                                         |
| Custom Spreadsheets    | Creation of makeshift Excel trackers or offline databases to bypass slow, official Electronic Health Record (EHR) workflows.                                                                                                                                |
| Needs v Wants          | Providers and staff see unsanctioned tools and are driven by desire to reduce administrative burdens. These can be legitimate needs due to gaps in capabilities. There are illegitimate wants stemming from not liking or understanding existing solutions. |
| File Sharing           | Clinical staff use personal Dropbox, Google Drive, or Microsoft OneDrive accounts to transfer and store large imaging files (e.g., DICOM files) or patient documents because institutional systems are deemed too cumbersome                                |
| Ease of Access/Use     | Staff implement/rely on unapproved external platforms for tracking patient appointments to reduce backlogs, bypassing official integrations.                                                                                                                |

# The IT Perspective: Why IT Cares So Much

IT is not trying to block progress – IT is trying to protect patients, clinicians, and the mission

## Cybersecurity & OPSEC

- Shadow IT bypasses mandatory cybersecurity controls and ATO processes
- Every unauthorized device emits signals that adversaries can detect and exploit
- Signals can be used to geolocate and kinetically target deployed units
- No patch management means known vulnerabilities remain unaddressed

## PHI & HIPAA Compliance

- Personal email, text, and apps transmit PHI outside of secured channels
- Significant HIPAA violation risk with potential civil and criminal penalties
- Unapproved systems lack SLAs and MOU/MOAs and audit trail for PHI access, transmission, or storage
- Breach notification obligations triggered by any unauthorized PHI disclosure

## Data Integrity & Accountability

- Encounters documented at incorrect locations create false medical records
- Downstream billing, reporting, and administrative errors cascade across systems
- Adverse event documentation may be inaccurate, complicating investigations
- No disaster recovery or backup for data stored in Shadow IT systems

# Bridging the Gap: Mutual Understanding is the Foundation

## CLINICAL PERSPECTIVE

- I need tools that work NOW
- My patients cannot wait for an ATO
- Approved systems create gaps in my workflow
- I did not know this was a problem
- I am trying to deliver the best care possible

## IT PERSPECTIVE

- Unapproved tools create cybersecurity risk / can negatively impact clinical decision-making
- HIPAA violations carry serious consequences
- We cannot protect what we cannot see
- Inaccurate records harm patients and missions
- We want to say YES - help us help you

**MUTUAL  
UNDERSTANDING**

When clinical teams and IT understand each other's WHY - real solutions become possible.

# Real-World Examples of Shadow IT in MTFs

|                                   |                                                                                                                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Warrior Eye Clinic</b>         | An Access database built locally to manage screening and appointments – operating outside of any approved system lifecycle or oversight.                                  |
| <b>Occupational Health</b>        | Apps not connected to MEDCOI where staff use personal hotspots and personal email to transfer patient data – creating uncontrolled PHI exposure.                          |
| <b>AI-Assisted Ortho System</b>   | An orthopedic team acquired an AI system to assist with hip replacements by analyzing patient images – procured without HI or IMD review.                                 |
| <b>Signal &amp; Personal Text</b> | Using consumer messaging apps and personal text messages to communicate patient information instead of approved, secure military platforms.                               |
| <b>Remote MHS GENESIS</b>         | Clinicians in Poland logging into MHS GENESIS using a stateside MTF location – creating false encounter location records with downstream billing and adverse event risks. |
| <b>Urology Clinic</b>             | Clinical staff in Urology clinic utilized Google Calendar for scheduling purposes in lieu of vetted and approved Amion application.                                       |

# The MHS GENESIS Documentation Problem

Scenario: A clinical team deployed in Poland logs into MHS GENESIS and documents a patient encounter using their home MTF location.

## Why This Matters:

- The encounter record incorrectly shows the patient was seen at the stateside MTF - not the actual deployed location
- Downstream billing errors: claims submitted for services rendered at incorrect facility
- Flawed reporting: readiness data, workload metrics, and clinical reporting become inaccurate
- Administrative consequences: staffing, resource allocation, and mission reporting become unreliable
- Adverse Event Risk: if a negative outcome occurs, documentation does not reflect actual circumstances, complicating investigation and accountability
  - Risk of inappropriate disclosure of Service Member death outside normal chain of Command
- Legal and compliance exposure: inaccurate records may conflict with witness accounts or other documentation

# Strategies for Mitigation

## Safe Sandboxes

Provide secure, governed, pre-approved digital environments where staff can experiment with new tools without risking patient information or organizational data/systems.

## Improve Approved Tools

Streamline the official EHR and IT workflows so the sanctioned path is the easiest path to take.

## Continuous Monitoring

Deploy Data Loss Prevention (DLP) to enforce PHI policy and detect unsanctioned data exfiltration.

## A Path to “Yes”

Develop enterprise-wide strategies that support innovation governance, rather than simply prohibiting new tools. Create an accessible entry point where applications and technologies can be submitted to J6 for review and evaluation.

# The 80 Percent Solution: Working Towards Yes

The 80% Solution: A practical, achievable outcome that meets most user needs while maintaining compliance - rather than demanding perfection before acting.

**Instead of NO...**

- Outright rejection of user tools
- No engagement with clinical teams
- Waiting for perfect solutions
- Treating all Shadow IT as malicious

**Ask WHY, Then...**

- What need/gap is this tool solving?
- What gap exists in approved systems?
- What risk(s) is the user accepting?
- How long has this been in use?

**Work Towards YES...**

- Bring tools into lifecycle management
- Apply cybersecurity best practices
- Collaborate through ISC & committees
- Find and implement approved alternatives together

**Meeting clinicians at their level and walking with them toward a safer solution is the mission.**

# Lifecycle, Engagement & Change Management

## Lifecycle Management

- Identify and catalog existing Shadow IT across all departments
- Evaluate risk, compliance, and operational value of each system
- Incorporate vetted tools into the formal system lifecycle process
- Establish ongoing monitoring, review, and refresh cycles

## User Engagement???

Get them to table / IMGC  
Innovation Committee

- Engage clinical teams early and often - seek to understand the WHY
- Create a culture of openness, not punishment, for disclosure
- Partner with department champions to bridge IT and clinical gaps
- Use ISC and committee structures to surface and address Shadow IT

## Change Management

- Communicate the risks of Shadow IT without blame or judgment
- Provide clear, simple pathways to request and adopt approved tools
- Celebrate wins when clinical needs are met through approved solutions
- Measure adoption continuously and adjust strategies as needed

# DHA Lines of Effort Alignment

**LOE 1**

## **Deliver Medically Ready Warfighters**

By addressing Shadow IT, we ensure secure and reliable IT systems that directly support warfighter readiness. Eliminating hidden risks protects the data infrastructure that clinical teams depend on.

**LOE 2**

## **Deliver Medical Warrior Currency**

Educating clinicians and informaticists on Shadow IT risks builds currency in health IT governance, cybersecurity awareness, and responsible technology use.

**LOE 3**

## **Deliver Joint Warfighting Capabilities**

Enhancing interoperability and reducing unauthorized system use ensures that joint clinical data flows accurately and securely across the enterprise.

**LOE 4**

## **Deliver the Healthcare Enterprise All Beneficiaries Deserve**

Addressing the root causes of Shadow IT improves IT governance, protects patient data, and ensures beneficiaries receive safe, accurately documented care.

# Call to Action

Use your ISC and existing committee structures to identify Shadow IT - then collaborate with clinical stakeholders to implement best practices and bring these systems into a monitored, compliant environment.

- 1 IDENTIFY: Conduct a Shadow IT assessment across all departments at your MTF
- 2 LISTEN: Meet with clinical end-users - ask WHY they are using unapproved tools without judgment
- 3 EVALUATE: Assess risk, compliance, and operational value of each identified system
- 4 COLLABORATE: Partner with HI, IMD, and ISC to develop a compliant path forward
- 5 ACT: Implement lifecycle management, cybersecurity controls, and HIPAA safeguards
- 6 SUSTAIN: Build a culture of shared responsibility - working together towards YES

# Knowledge Check (1 of 3)

## Question 1 (Multiple Choice)

What is the PRIMARY reason clinical end-users adopt Shadow IT solutions?

- 1 To intentionally bypass IT security controls
- 2 To deliver better, faster patient care when approved tools have gaps
- 3 To reduce their personal workload
- 4 To avoid accountability for their actions

# Knowledge Check (2 of 3)

## Question 2 (Multiple Choice)

What is a key benefit of the 80 percent solution in managing Shadow IT?

- 1 Complete elimination of all Shadow IT immediately
- 2 Strict enforcement of IT policies without user input
- 3 Balancing clinical user needs with IT compliance and security
- 4 Ignoring Shadow IT until it becomes a larger problem

## Knowledge Check (3 of 3)

### Question 3 (True / False)

Understanding the clinical WHY behind Shadow IT usage improves collaboration between users and IT

TRUE

# Contact Information

**MAJ(P) Danial H. Lister, MSN, BSN, BC**  
Chief of Medical Management,  
Evans Army Community Hospital

 daniel.h.lister.mil@health.mil

---

**Ms. Yolanda J. Farmer**  
CIO, Womack Army Medical Center

 yolanda.j.farmer.civ@health.mil

**MAJ(P) Adam O. Rich, MS, RN**  
CHIO, Womack Army Medical Center

 adam.o.rich.mil@health.mil

---

**Mr. Kirby J. Lyford**  
CIO, Landstuhl Regional Medical Center

 kirby.j.lyford.civ@health.mil

# Copyright Statement

*“We are military service members and employees of the U.S. Government. This work was prepared as part of our official duties. Title 17, U.S.C., Section 105 provides that copyright protection under this title is not available for any work of the U.S. Government. Title 17, U.S.C., Section 101 defines a U.S. Government work as a work prepared by a military service member or employee of the U.S. Government as part of that person's official duties.”*

# 2026 DEFENSE HEALTH INFORMATION TECHNOLOGY SYMPOSIUM

August 11-13, 2026  
Hyatt Regency New Orleans  
New Orleans, LA

# Thank you!

UNCLASSIFIED

UNCLASSIFIED



2025 DHITS 25