Military Cyber Affairs

Volume 6
Issue 1 *HammerCon 2023 Issue*

Article 5

May 2023

Combining Frameworks to Improve Military Health System Quality and Cybersecurity

Dr. Maureen L. Schafer
Georgetown University, mls374@georgetown.edu

Dr. Joseph H. Schafer
National Defense University, College of Information and Cyberspace, joseph.schafer@milcyber.org

Combining Frameworks to Improve Military Health System Quality and Cybersecurity

Cover Page Footnote

The authors wish to acknowledge their students and colleagues at Georgetown University, the George Washington University, and the National Defense University whose discussions enrich these ideas.

Combining Frameworks to Improve Military Health System Quality and Cybersecurity

Dr. Maureen Lucy Schafer and Dr. Joseph Hughes Schafer

Introduction

Existing conceptual frameworks and commercially available technology could be considered to rapidly operationalize the use of Quality Measures (QM) within military health systems (Costantino et al. 2020). Purchased healthcare as well as digital healthcare services have paved the way for data collection from multiple information systems thus offering stakeholders actionable intelligence to both guide and measure healthcare outcomes. However, the collection of data secondary to Smart Devices, disparate information systems, cloud services, and the Internet of Medical Things (IOMT) is a complication for security experts that also affect clients, stakeholders, organizations, and businesses delivering patient care. Health care is the only industry globally for which the biggest threat to data breaches comes from internal sources, and security experts recommend that a framework approach in this domain with analysis of data breaches provides insights into analyzing and forecasting the data breaches (Seh et al. 2020).

Inspired by the combined efforts of these and other scientists, the authors propose the application of three combined quality frameworks to guide methodology and provide a useful tool to support the Department of Defense (DoD) Military Health Systems' (MHS) purchased healthcare component. The aim of this adapted framework is to provide a secure QM tool that will (1) assess and prioritize clinical quality indicators, and to (2) establish consistent performance standards and requirements that align with DoD Information Security standards between the MHS QM to their purchased care providers. Deployment of such a framework may enhance secure data quality capture and analyses, and provide quality outcomes data back to Defense Health Agency (DHA) stakeholders. Successful framework application may use leading indicators such as predictive measurements to strengthen patient outcomes in an applied research environment.

Today, federal healthcare organizations are increasingly both valued and held accountable for transparency, connectivity, security, and quality outcomes at the highest levels of our government. The effectiveness, efficiency and reliability of the DHA services is then reliant on the quality of data in health information systems accessed by patients, providers, researchers, and stakeholders. DHA offers information technology (IT) tools as part of the DoD Medical Community of Interest (Med-COI) while also leveraging the Desktop-to-Datacenter (D2D) program. Med-COI is a single, enterprise-wide network designed to support

military health IT requirements, while D2D supports the standardized delivery of enterprise services specifically enabling providers and staff access to the applications via any clinical desktop in any Military Treatment Facility (MTF). The challenge is that the DoD through DHA operates one of the largest health care systems in the United States with a unique and honored mission, and quality is a perception of the level of value customer places on the DHA outputs, along with the degree to which these meet established quality and security specifications and benchmarks per DoD.

Everything DHA does impacts quality from cultural transformation (e.g., oversight to ensure safe, high-quality care), to information technology (IT) implementation and operations and/or creating specialized health systems functions (e.g., research, knowledge translation, and Clinical Practice Guidelines (CPG) implementation) as well as ensuring cybersecurity. Based on guidance from The Joint Commission (TJC), and their own mission needs, DHA requires clinical quality indicators across their direct and purchased care sectors. TRICARE is the purchased care network that provides healthcare services to DHA's beneficiaries (Bond and Schwab 2019). Secondary to the varied structure and processes used by the multitude of purchased care components, accurate measurement of the quality of care provided for DoD beneficiaries is difficult to achieve. Additionally, these networks participate in disparate quality programs such as Agency for Healthcare Research and Quality (AHRQ), TJC, National Committee for Quality Assurance (NCQA), and the Hospital Compare program. Providing the purchased care networks with a secure framework for data collection, submission and reporting to TRICARE may offer quality measures that are grouped into user-friendly dashboard versions that demonstrate measures more clearly (Randell et al. 2019). This approach meets recommendations regarding use of a conceptual framework and leverages current IT such as a dashboard to rapidly operationalize the use of QMs in the MHS (Costantino et al. 2020).

Frameworks

A conceptual framework provides a common language, guiding principles, and supports an evidence-based approach (Varpio et al. 2020) to an enquiry within that said domain. For instance, quality conceptual frameworks directly identify important indicators (i.e., context (policy, laws, accreditation), best practices, and Stakeholder's (Congress, DoD, DHA, and patient) priorities, and guides synthesis of the collected evidence to support healthcare organizations in identifying successful domain measures, as well as existing gaps when assessing their quality performance measures.

To meet the aims of this paper, the authors have combined three conceptual frameworks:

1. Donabedian's Quality Attributes (DQA) Framework.

2. The National Academy of Medicine (NAM) Framework.

3. Healthcare and Public Health (HPH) Cybersecurity Framework (HCF).

Each of these frameworks is well-tested, widely accepted, and referenced as the gold standard in delivering quality care (DQA and NAM) and cybersecurity (HCF) for healthcare. Separately, each framework provides long-used analysis, guidance, and application of quality reliable measures of healthcare services. The combined frameworks may enhance data integrity (collection and standardized safety of data in regard to regulatory compliance). The combined frameworks also support the identifying gaps in quality of care, support the prioritization of cost-effective methodologies that predictably improve patient outcomes, and support DHA's quality measures. Finally, the authors offer the importance of understanding the components of quality measures in a more precise manner while maintaining IT governance compliance.

Donabedian's Quality Attributes Framework

Donabedian's three domains (Ayanian and Markel 2016) of focus are organized into Structure, Process, and Outcome - a meaningful order, and representative of DHA's performance quality indicators.

1. Structural Measures - refer to quality measures at the system and provider level, such as attributes of the settings in which care is provided. It includes such elements as resources, staff and equipment material resources, facilities, equipment, human resources, and organizational structures.
2. Process Measures - covers all aspects of delivering care and is related to interaction within and between practitioners and patients to include adherence to policy, standards, and procedures.
3. Outcome Measures - the effect of care and its impact on the health status of patients and populations**.** There are three essential measurements (Protti 2009) achieved through smart data capture that result in outcomes of *transparency, integrated care, and interoperability*.

Knowledge of the linkage between Donabedian's three constructs is critical in reaching the intent of quality performance measures. Policy, standards, and procedures both guide and hold accountable healthcare organizations. Well-planned and executed structures and processes has been shown to improve outcomes, effect of care, and health status of patients and populations (Birkland 2019, 94–97).

The National Academy of Medicine Framework

The NAM Framework (formerly the Institute of Medicine (IoM) Framework) quality attributes identify the fundamental domains that need to be addressed to

improve the healthcare services delivered to individuals and populations (Institute of Medicine 2001, 233–35). The NAM framework notes six attributes to gauge inconsistent care across a healthcare system and to meet quality care outcomes. They are labeled as: (1) Effective, (2) Efficient, (3) Safe, (4) Timely, (5) Patient-Centered, and (6) Equitable. As such, the six attribute definitions within this framework are self-explanatory and are described briefly in Table 1 (i.e., column 1). Application of these attributes support the care of patients (i.e., MHS purchased care) to be fundamentally improved, offer an understanding of the current care environment, the existing evidence base, the opportunities for improvement, and the documentation of the improvements needs to be realized. (Iglesia, Greenhawt, and Shaker 2020). The NAM's Six Aims provide a useful framework to advance the quality of care across the MHS purchased care population.

Healthcare and Public Health (HPH) Cybersecurity Framework (HCF)

In March 2023, the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group and the U.S. Department of Health and Human Services (HHS) jointly released a Cybersecurity Framework Implementation Guide (CFIG). This joint public-private partnership for critical infrastructure protection also included The National Institute for Standards and Technology (NIST) and other federal agencies. The guide aims to help HPH organizations align their cybersecurity programs with the current NIST Cybersecurity Framework and related guidance.

HPH Cybersecurity (HCF) Background

The healthcare system is a national critical infrastructures identified by the U.S government in 1998 to establish public-private partnerships for critical infrastructure protection (Clinton 1998). The U.S. Department of Homeland Security established the Healthcare and Public Health (HPH) Sector as a critical infrastructure sector in 2003. The security and resilience of the HPH are essential to national security, the economy, and public health and safety. The 2016 HPH Sector-Specific Plan (SSP) reflects the maturation of the partnership and the progress from the earlier 2007 and 2010 HPH SSPs (CISA 2016, 2).

The HPH SSP details how the National Infrastructure Protection Plan risk management framework (CISA 2013) is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector Risk Management Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Department of Health and Human Services (HHS) is designated as the Sector Risk Management Agency for the HPH Sector (CISA 2016, 14). HHS recognizes the HSCC Cybersecurity Working Group as an advisory body organized under the NIPP.

Cybersecurity Framework Implementation Guide (CFIG)

The CFIG provides specific steps that healthcare organizations can take immediately to manage cyber risks to their IT systems and reduce the number of cyber incidents affecting the sector (HSCC and HHS 2023).

The NIST Cybersecurity Framework is a risk management model that has become the standard for government agencies and industry in managing cybersecurity risks (NIST 2018) which is the foundation for the CFIG. With the CFIG, healthcare organizations can assess their current cybersecurity practices and risks and identify gaps for remediation, Such as:

- Steering risk management best practices;
- Sharing a common lexicon for cybersecurity risk;
- Outlining a cybersecurity risk management structure;
- Identifying cost-effective cybersecurity management standards.

Recent high-profile cyberattacks reinforce the need for health organizations to improve cybersecurity; More than 50 million U.S. patient records were compromised in 2022 ("Horizon Report: The State of Cybersecurity in Healthcare" 2023, 4). In November 2022, Senator Mark Warner released a report, Cybersecurity is Patient Safety: Policy Options in the Health Care Sector which states:

> The health care sector is vulnerable to cyberattacks for a number of reasons, including its reliance on legacy technology, a wide and highly varied attack surface (that only grows more complex from the ever-increasing number of connected devices), a high-pressure environment where even the slightest delay can have life-or-death consequences, funding constraints, and an outdated mode of thinking that views cybersecurity as a secondary or tertiary concern (Warner 2022, 36).

Addressing this issue requires a concerted effort, not only to clarify frameworks but also to increase understanding of cybersecurity. Intensifying the urgency, the U.S. Securities and Exchange Commission (SEC) has proposed rules that will require cyber expertise on governing boards along with additional cybersecurity breach and resiliency disclosures from regulated entities (SEC 2022); adoption is expected soon. The alternative is to face substantial reputational and financial loss and most importantly to risk patients' lives.

Operationalizing the combined MHS Cybersecurity and Quality Measures Frameworks

The authors will refer to the combined three frameworks (DQA, NAM, & HCF) as the MHS Cybersecurity and Quality (MCQ) Framework with the end goal of providing structure to accommodate HPH-specific aspects of cybersecurity while also supporting quality healthcare service delivery. The MCQ essentially acts as a dashboard view of both in the MHS purchased care population. As depicted in Table 1, it offers examples of measures that align across and down within the combined frameworks. Not all Quality Indicators will necessarily meet each of the MCQ Framework attributes, but it may more clearly measure cybersecurity efforts, and offer a QM based on the number of attributes achieved in the framework, highlight potential gaps, and support the standardized generation of MCQ criteria which are measurable, meaningful, and manageable across all providers. Essentially, it becomes a common shared tool to guide all providers to meet the DoD's Cybersecurity requirements and the DHA QM standards (i.e., network providers) to enhance data integrity and value-based performance within the MHS.

The MCQ Framework highlights gaps, and allows for recommendations: patient prescription compliance; provider practice and satisfaction reporting; cultural awareness training; safety alarms in place to identify noncompliance; optimal coordination of resources; cost of service analysis; total system response time; and comprehensive patient prescription analysis. Notwithstanding these gaps, there is reasonable consistency in many of the measures used and mapped against the DHAs QMs (Williams et al. 2019), and DoD's cybersecurity requirements.

The proposed MCQ Framework builds upon established cybersecurity and core healthcare quality criteria which are measurable, meaningful, and manageable. In a dynamic, healthcare context such as the DoD, the framework provides DoD governance requirements structure to accommodate specific aspects of DHA healthcare service delivery: prioritizing cybersecurity attributes; quality measures common for both direct and purchased care that expand the range of quality areas covered by the measures; and establishing consistent performance standards and corrective action requirements for direct and purchased care providers.

	Donabedian **Structure**	Donabedian **Process**	Donabedian **Outcome**
NAM Attributes	HPH Cybersecurity Framework Attributes		
Effective Providing services based on scientific knowledge	IT infrastructure, personnel, expertise, facilities, equipment, and funding **Example:** Provider to Patient Staff Ratio (Acuity)	Appropriate & timely guidelines and training **Example:** medication refills	Mandatory staff training Improved patient survival **Example:** Mortality: alive/dead Impairment: pathology, clinical measures
	budget meets organizational cybersecurity needs	100% staff are trained credentials & licensing	25% decrease in phishing attacks
Efficient Relates the cost of healthcare to the outputs or benefits obtained	Appropriate systems, facilities, HR, equipment, or funding; minimize waste of equipment, ideas, or energy **Example:** HEDIS admission: Coordination, protocol staff, equipment, building	CPGs and policy support appropriate tasking to healthcare mission **Example:** Pathway of Care-Optimal coordination of healthcare resources	Decrease in malware/phishing Decrease in patient mortality and morbidity **Example:** Effects of direct care costs to patient
	usability and reliability re telehealth, IOMT, mobile devices	built for sustainability, open standards, open data, open source, open innovation	diminished liability, low vulnerable IOMT, telehealth & mobile devices
Safe Data integrity, Avoiding organizational and patient injury	System safety indicators in place for upward utility trends. **Example:** clinical team composition meets the needs of the MTF patient population	Responsiveness of Service (compliance to established cybersecurity and clinical standards) **Example:** Patient records, treatment plans, information	Patient survival; avoiding adverse events **Example:** Disability: functional status Acceptability
	quality, role based, access, consent, and privacy	legal, ethical, & information confidentiality standards & issues implemented	DoD cybersecurity guidelines achieved
Patient Centered	Accessibility to Service **Example:** outpatient wait times for routine appointments	Access to definitive interventions **Example:** wait time (i.e., routine, acute etc.)	Patient satisfaction and comfort **Example:** *HCAHPS*
	HITECH, HITRUST, ONC, FDA certified	access, usability, and language barriers supported across information systems	care quality-permitted purposes, permitted users full participation
Timeliness data via systems and IT reduces delays for those that give and receive care	Accessibility of Service **Example:** Population management and use of Patient Centered Medical Home	Responsiveness of Service *(service time intervals)* **Example:** prescription practices	Morbidity & Mortality **Example:** Reduction in acute asthma exacerbation
	data standardization	data integrity leads to meaningful information	assurance of information & knowledge
Equitable fair distribution of healthcare	Accessibility of Service **Example:** Demographic (Med Evac, Transfer), Cultural awareness and sensitivity	Patient Disposition **Example:** Referral System (identify steps)	Disparate Mortality Rates **Example:** Patient, & community satisfaction & follow-up
	Analyze & Prioritize: Users, Regulations, Principles, Technical requirements, testing requirements, policies, governance structure, accountability measures, process for adding & changing requirements.		

Table 1. MHS Cybersecurity & Quality (MCQ) Framework

About the Authors

Maureen Lucy Schafer, Ph.D.
Adjunct Professor, Georgetown University

Dr. Maureen L. Schafer is a Clinical Informaticist, Licensed and Board-Certified Family Nurse Practitioner (FNP), and Georgetown University Professor with expertise in the application of health care systems and information technology across the clinical care continuum. She has a BSN (RN) from St. Joseph's College, MSN (FNP) from The Catholic University of America, and a Ph.D. (Health Systems and Informatics) from the University of Arizona. Upon completion of her military career as an Army Nurse, she continued to lead and improve lives as a professor at George Mason University, and within industry as a Practice Leader for Telligen, DLH, and Philips. Currently, with two appointments at Georgetown University, she guides and mentors' students across the curriculum to turn research into action solving challenging healthcare problems teaching three courses: Informatics, Technology & Quality (School of Nursing and Health Studies), Health Informatics, and Information Systems (Department of Health Systems Administration).

Joseph Hughes Schafer, Ph.D.
Professor, National Defense University, College of Information and Cyberspace

Dr. Joseph H. Schafer is a Professor at NDU's College of Information and Cyberspace where he served as Department Chair and Associate Dean. After his Army career, he served as an executive at Dell and Vice President of L3. He has acquired and operated telecommunications, information, and cybersecurity systems in Iraq, the White House, and the Pentagon. He has a B.S. in Electrical Engineering & Computer Science from West Point; M.S. and Ph.D. in Computer Science from GWU; M.A. in Strategy from Naval War College; and M.B.A. from UVA Darden. He holds CISSP, CEH and QTE certifications and serves on several boards. He has taught in GWU's Cybersecurity M.S. since 2014. At NDU Joseph teaches U.S. and allied Cyber Workforce and War College students. He developed and teaches the Artificial Intelligence and National Security course. Dr. Schafer is currently creating the Framework for National Security Cyber Policy.

Acknowledgement

We wish to acknowledge our students and colleagues at Georgetown University, the George Washington University, and the National Defense University whose discussions enrich these ideas.

References

Ayanian, John Z., and Howard Markel. 2016. "Donabedian's Lasting Framework for Health Care Quality." *New England Journal of Medicine* 375 (3): 205–7. https://doi.org/10.1056/NEJMp1605101.

Birkland, Thomas A. 2019. *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making*. 5th edition. New York: Routledge.

Bond, Amelia M., and Stephen D. Schwab. 2019. "Utilization Variation In Military Versus Civilian Care: Evidence From TRICARE." *Health Affairs* 38 (8): 1327–34. https://doi.org/10.1377/hlthaff.2019.00298.

CISA. 2013. "National Infrastructure Protection Plan (NIPP)." Washington, DC: Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan.

———. 2016. "Healthcare and Public Health Sector Specific Plan." Washington, DC: Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector.

Clinton, William Jefferson. 1998. "Protecting America's Critical Infrastructure." PPD 63. Presidential Decision Directive/NSC-63. Washington, DC: The White House.

Costantino, Ryan C, David Nau, Jeffrey J Neigh, Paul J Hoerner, Jessica R Hull, and Eleanor Perfetto. 2020. "Use of Pharmacy Quality Measures to Enhance Value-Based Performance Within the Military Health System." *Military Medicine* 185 (5–6): e894–99. https://doi.org/10.1093/milmed/usz435.

"Horizon Report: The State of Cybersecurity in Healthcare." 2023. Franklin, TN: Fortified Health Security. https://fortifiedhealthsecurity.com/pressreleases/fortified-health-security-releases-2023-horizon-report/.

HSCC and HHS. 2023. "Healthcare and Public Health (HPH) Sector Cybersecurity Framework Implementation Guide V2." Washington, DC: Health Sector Coordinating Council (HSCC) Cybersecurity Working Group and the U.S. Department of Health and Human Services (HHS). https://aspr.hhs.gov:443/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx.

Iglesia, Edward G. A., Matthew Greenhawt, and Marcus S. Shaker. 2020. "Achieving the Quadruple Aim to Deliver Value-Based Allergy Care in an Ever-Evolving Health Care System." *Annals of Allergy, Asthma & Immunology* 125 (2): 126–36. https://doi.org/10.1016/j.anai.2020.04.007.

Institute of Medicine. 2001. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academies Press. https://doi.org/10.17226/10027.

NIST. 2018. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." NIST Cybersecurity White Paper CSF v 1.1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018.

Protti, Denis. 2009. "Integrated Care Needs Integrated Information Management and Technology." *Healthcare Quarterly* 13 (sp): 24–29. https://doi.org/10.12927/hcq.2009.21093.

Randell, Rebecca, Natasha Alvarado, Lynn McVey, Roy A Ruddle, Patrick Doherty, Chris Gale, Mamas Mamas, and Dawn Dowding. 2019. "Requirements for a Quality Dashboard: Lessons from National Clinical Audits," November.

SEC. 2022. "Public Company Cybersecurity; Proposed Rules." Release # 33-11038. Washington, DC: Securities and Exchange Commission. https://www.sec.gov/file/33-11038-fact-sheet.

Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. 2020. "Healthcare Data Breaches: Insights and Implications." *Healthcare* 8 (2): 133. https://doi.org/10.3390/healthcare8020133.

Varpio, Lara, Elise Paradis, Sebastian Uijtdehaage, and Meredith Young. 2020. "The Distinctions Between Theory, Theoretical Framework, and Conceptual Framework." *Academic Medicine* 95 (7): 989. https://doi.org/10.1097/ACM.0000000000003075.

Warner, Mark R. 2022. "Cybersecurity Is Patient Safety: Policy Options in the Health Care Sector." Washington, DC: United States Senate. https://www.warner.senate.gov/public/index.cfm/2022/11/warner-releases-policy-options-paper-addressing-cybersecurity-in-the-health-care-sector.

Williams, Arthur Robin, Edward V. Nunes, Adam Bisaga, Frances R. Levin, and Mark Olfson. 2019. "Development of a Cascade of Care for Responding to the Opioid Epidemic." *The American Journal of Drug and Alcohol Abuse* 45 (1): 1–10. https://doi.org/10.1080/00952990.2018.1546862.