Balancing Patient Safety, Clinical Efficacy, and Cybersecurity with Clinician Partners

Joseph Schneider and Axel Wirth

***Joseph Schneider**, MD, MBA, is an assistant professor at the University of Texas Southwestern in Dallas, TX. Email: drjoes1tx@gmail.com*

***Axel Wirth**, CPHIMS, CISSP, HCISPP, AAMIF, FHIMSS, is the chief security strategist at MedCrypt in San Diego, CA. Email: axel@medcrypt.co*
Corresponding author

Where We Stand Today

Cybersecurity events affecting healthcare organizations are in the news with increasing frequency, indicating their growing impact and expanse.[1] We have seen incidents ranging from breaches affecting millions of patient records to attacks shutting down hospitals across the country,[2] with at least one of them tragically contributing to the death of a patient.[3] Most recently, the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Department of Health & Human Services (HHS) issued a joint warning about the healthcare industry being a target of expanding ransomware activity.[4] Meanwhile, ransom financial demands are rising[5] and adversaries are resorting to increasingly brazen methods, including exfiltrating data and extorting patients.[6]

COVID-19 has accelerated the trend toward connectivity in healthcare. We have added remote workers and remote patients using telehealth services and are placing devices in patients' homes, offering a wide range of attack opportunities as critical data are transmitted across home and public networks. Healthcare is now taking place in a much more complex and highly accessible space, offering rich data and a growing attack surface.

With the rapidly evolving, increasingly connected information technology (IT) infrastructure and growth of cyberthreats, healthcare is facing a perfect storm. The danger is exacerbated by the fact that we are no longer dealing solely with individual hackers but mainly with well-resourced cybercriminal organizations, as well as politically and economically motivated adversaries (e.g., nation-states, cyber terrorists). Global economic losses due to cyber incidents are estimated to be in the $3-trillion range and are expected to reach $6 trillion in 2021 and $10.5 trillion by 2025.[7] Healthcare organizations are expected to spend $125 billion on cybersecurity over the next 5 years.[8]

It is imperative that healthcare improve its cyber defenses and "cyber culture." This includes expanding our understanding of cyber risks, better defining what we must protect, learning how to protect it in ways that support efficient workflows and safety, and instilling good user cyber behavior. IT security and clinical engineering cannot do this alone.

To develop a safe and effective path forward, we also need cyber-savvy clinicians working as partners to ensure that clinical needs are met in security decisions. This article proposes an approach and explores how we might achieve this.

The Changing Healthcare Cybersecurity Paradigm

Healthcare organizations are easy targets for cyber adversaries because of their complexity, security weaknesses, and many available entry points. The information they hold is rich and has long-term value. This includes patients' health data, financial and insurance data, and intellectual property (e.g., medical research, designs and formularies, software algorithms, proprietary business data).[9]

Although stolen health information usually is valued relatively highly in the underground economy, it sometimes can be difficult to monetize, requiring skill and patience. We occasionally have seen "fire sales" or even free data dumps of health data.[10] The attractiveness of healthcare information continues to be strong, but pricing—meaning the opportunity for the cybercriminal to make a profit—may vary widely.

Examples for motivations for healthcare attacks range from monetary gain (e.g., data theft and subsequent extortion attempts by organizations such as The Dark Overlord)[11,12]

to the desire to make a political statement (e.g., denial-of-service attacks on the Boston Children's Hospital[13] and Hurley Medical Center in Flint, MI[14]). Healthcare organizations also have been particularly hard hit by ransomware attacks, as the pressure to restore healthcare services leads to willingness to give in to demands.[15]

Recent cyber incidents have demonstrated the complex and severe consequences that such events can have on health and safety. In 2017, WannaCry shut down 81 of 236 U.K. National Health Service hospitals[16] and NotPetya led to steep financial losses for a pharmaceutical company and affected availability of drugs and vaccines.[17] Estimates put the global financial damage of WannaCry in the $4- to $8-billion range and NotPetya above $10 billion.[18] Success in law enforcement is rare, and attackers seldom are prosecuted, though occasionally justice prevails.[19]

Many attacks benefit from systemic weaknesses, such as legacy systems that are no longer supported by the manufacturer. Other systemic risks can result from delayed deployment of the many software "patches" we need to manage or the complexity and difficulty of upgrading firmware of medical devices in coordination with clinical operations and care delivery.

In addition to requiring a holistic and integrated approach to applying security technologies, the new security paradigm requires cultural and organizational change. Everyone, no matter their role, needs to be aware of today's cyber risks and needs to contribute to improving their organization's security posture and averting security compromise. This affects everything from how we use systems and devices, to our vendor and partner relationships, to procurement decisions, and to replacement planning. Cybersecurity has become a multidisciplinary approach, including not only traditional IT and IT security roles, but also everybody from the boardroom to the clinical caregiver.

Clinician Involvement in the New Paradigm

Clinicians often perceive cybersecurity decisions as being made without recognition of the need for safe, timely, efficient, effective, equitable, and patient-centered care (STEEEP). (STEEEP denotes the Institute of Medicine's six aims. It was originally coined and trademarked by the Baylor Health Care System [now Baylor Scott and White].) As a result, clinicians often perceive cybersecurity requirements as a burden. Cybersecurity education designed by nonclinicians frequently is perceived as an attempt to scare and often fails to motivate clinicians appropriately. As Mark Jarrett, MD, noted in an article for *JAMA*, "Physicians, as well as others in the health care industry, have historically considered IT issues as an IT problem."[20]

This viewpoint has started to change as cyberattacks have become more common and have affected patient care. A survey conducted in 2017 by the American Medical Association (AMA) and Accenture found that 83% of the 1,300 physician respondents had experienced a cyberattack.[21] More than one-half of respondents reported being "very worried" about future attacks and having concerns about patient safety, while 74% were concerned about electronic health record (EHR) security issues, including compromised patient data.

The AMA and others have made it clear that cybersecurity is a safety issue. It can interrupt or interfere with care, as well as sap resources that are needed in other areas. AMA past-president David Barbe, MD, said, "Cybersecurity isn't just a technical and policy issue; it's a patient safety issue. ... If physicians don't have access to their records—patient histories, what medications they're on—it will be difficult to provide appropriate care."[22]

This view was underscored at a Food and Drug Administration (FDA) Patient Engagement Advisory Committee meeting, where participants stated that "cyber training ought to be increasingly incorporated into medical, pharmacy and nursing school curriculums, particularly in device-heavy specialties like cardiology or nephrology" and concluding that the "US needs cyber-savvy doctors as connected device use rises."[23]

Despite the increasing awareness that cybersecurity is a patient safety issue, we have seen only a handful of attempts at

direct physician/clinician involvement in cybersecurity decision making. For example, the recommendations by Jarrett in his *JAMA* editorial[20] are helpful, but admonitions such as "individual clinicians must practice cyber hygiene" and "advocating for adequate resources is also important" will not improve the decision-making capabilities of technical stakeholders (e.g., IT security, clinical engineering). Unfortunately, clinician "advocacy" often takes the form of complaints because administrators may not know how to listen to physicians/clinicians and clinicians may not know how to engage administrators.

It seems clear that in most cases, the approach that we currently are taking (i.e., the virtual exclusion of physicians and other clinicians from all aspects of cybersecurity decision making) is not working.

Over the past years, we have seen scenarios that have highlighted the need for direct physician/clinician involvement in cybersecurity. Two examples are provided below.

In the first example, a medical device manufacturer issued a critical security update for an implantable life-supporting medical device. The alert was covered in the press and evening news.[24] Patients were advised to discuss with their physicians whether they should have their device's firmware updated. No national decision guidelines were provided to physicians to help them guide patients in making sensible decisions.

In such a situation, how should physicians advise their patients? How should they balance the clinical risk of the update against the cybersecurity risk posed by the vulnerability? Today, we lack the necessary risk models to support these decision processes. Going forward, these situations will become more frequent. Clinical cyber specialists can help develop such guidance and provide decision tools to the physician community and communications to patients to find the best approach to balancing safety, patient concerns, and cyber risk.

In the second example, a malware worm was introduced into the interventional cardiology catheterization laboratory and spread to several devices. The hospital's ability to perform cardiac cath procedures was severely hampered. Several emergency patients were en route, and a decision had to be made whether patients should be diverted to other facilities in the area.[25]

How should the cyber/clinical tradeoff be made to balance the risk to the remaining

Decisions about how to protect systems that affect clinical care are much too critical and complex to be made without clinical participation. Everyone in healthcare, regardless of their role, needs to be aware of today's cyber risks and must contribute to improving their organization's security posture and averting security compromise. IT security and clinical engineering cannot do this alone: Cyber-savvy clinicians working as partners are needed to develop a safe and effective path forward.

unaffected devices and the hospital's IT infrastructure against the medical needs of incoming patients? A cyber-educated clinician could help make that decision, balancing the potential for cyber harm versus clinical risks in both the planning and response to an incident.

These examples highlight the need for meaningful clinical versus cybersecurity tradeoff decisions and new ways of communicating about cyber risks with clinical stakeholders and ultimately the patient.

We feel that decisions about how to protect systems that affect clinical care are much too critical and complex to be made without clinical participation. Cybersecurity can be improved when decisions are made as a partnership between security-educated clinicians and security professionals that appropriately balance STEEEP and cybersecurity. We propose that this partnership can be best enhanced by identifying a lead clinical director of cybersecurity, as outlined below.

Role of the Clinical Director of Cybersecurity in the New Paradigm

Just as organizations are utilizing physicians and nurses who are specially trained in informatics to help with EHR and other informatics decisions, a qualified, well-respected, security-educated clinical director of cybersecurity can be a true partner with IT security and clinical engineering in cybersecurity decision making. Their primary function is to partner with IT security and clinical engineering internally and with vendors and cybersecurity experts externally in finding the right balance between cybersecurity and STEEEP.

The clinical director of cybersecurity should support an organization's capabilities and help develop best practices for the four pillars of an effective cybersecurity program (i.e., cyber awareness, cyber hygiene, cyber management, and cyber-incident response; sidebar on this page). The first two pillars are mainly organizational and procedural, whereas the latter two are more technical.

Specifically, this new healthcare cybersecurity paradigm should include the following, much of which can be responsibilities of the clinical director of cybersecurity:

- An organizational decision-making model should be established that spans the continuum of STEEEP and cybersecurity.
- The clinical organization and patient safety should be represented in all decisions regarding cybersecurity, including equipment life cycle planning, procurement decisions, and security workflows.
- Governance and clinically relevant education programs should be established, along with criteria for measuring the effectiveness of clinician understanding and involvement.
- "Cybersecurity rounds" should be conducted for visibility, education, and remediation of issues. These would be similar to "safety rounds," which have a demonstrated effectiveness.
- Processes and tools should be developed for reporting on the clinical aspects of cyber weaknesses and incidents.
- A clinician should act as an advocate and spokesperson for cybersecurity topics in the clinical community.
- When cyber-risk issues arise, there should be a lead clinical representative to patients, the clinical community, staff in IT security and clinical engineering, and the organization's leadership and board of directors.
- As part of the incident response process, a "command center" should be created for

Main Pillars of a Cybersecurity Program

- **Cyber awareness.** A user's knowledge, understanding, and attitude that help maintain an organization's cybersecurity posture.
- **Cyber hygiene.** User practices and behaviors that maintain cybersecurity and reduce an organization's security risk and exposure.
- **Cyber management.** Oversight and management of cybersecurity programs, technologies, and infrastructure.
- **Cyber-incident response.** Addressing and managing a security incident or cyberattack with the goal to minimize impact and optimize recovery time.

disseminating clinical guidance during cyber incidents.
- Clinical cyber-decision tools and best practices should be provided that support decision making in specific incidents, including decision trees to support clinical cyber-incident response (i.e., cyber triage).
- Engagement should occur with clinical cybersecurity professional organizations and initiatives on a regional and/or national level.

A summary of the responsibilities of the clinical director of cybersecurity is provided in Table 1.

Role	Responsibilities
Administrative	• Security strategy and governance • Procurement decisions • Replacement planning
Enablement	• Education • Peer leadership
Public	• Public representation • Communication • Patient advisory and advocacy
Security	• Security incident response • Security research

Table 1. Responsibilities of the clinical director of cybersecurity.

Benefits of a Clinical Director of Cybersecurity Role

An effective clinical director of cybersecurity can provide the benefits implicit in the responsibilities listed above. Less obvious benefits are that clinical users increasingly may understand that cybersecurity requirements are made with an understanding of the need for STEEEP. Because of this understanding, they can help reduce the risk of cyber compromise to IT equipment and medical devices by being more aware of risks and more engaged to help detect cyber incidents before they spread. This can be accomplished through reporting of unusual equipment or device behavior. Further, clinicians feeling that they are "a part of something" may help reduce burnout, which may be a cyber risk in its own right. Finally, physicians and other clinicians will be more receptive to requirements or changes that are brought to them by their peers, rather than by security professionals.

Identifying and Developing the Clinical Director of Cybersecurity Role

Finding physicians/clinicians willing to take on the cybersecurity responsibilities outlined above is not simple. Potential approaches include:
- Motivating a physician/clinician to make a change from their career pathway by convincing them of its potential to improve their organizational value through the development of leadership skills.
- Convincing nonclinical leadership that this position is valuable by illustrating the negative impacts of not having a clinically supported cybersecurity program.
- Identifying a candidate with the ability and desire to learn about the core technical aspects of cybersecurity and who can communicate clearly and effectively to both their clinical counterparts and to IT security and clinical engineering. These individuals increasingly are found in informatics programs, including fellowship graduates.

The following suggestions can help organizations find, develop, and retain these valuable individuals:
- **Organizational support:**
  - The clinical director position reporting relationship should be independent of IT security and clinical engineering.
  - The clinical director should cochair the organization's cybersecurity committee, with the ability to appeal decisions to the organization's senior leadership if they feel that patient safety is at risk.
  - The clinical director should be compensated for their time, which will vary with the complexity of the organization and the scope of the role.
  - Smaller organizations (e.g., smaller hospitals, individual physicians, group practices) may need to partner with larger organizations, including state medical associations, to provide these skills.
- **Experience and educational support:**
  - Although experience in cybersecurity is ideal, physicians/clinicians can learn on-the-job from the chief information

security officer, chief information officer, chief medical information officer (CMIO), clinical engineering cyber lead, and others.
- Additional education should be obtained through seminars, online classes, etc., provided by external professional organizations.
- A national standard curriculum should be created to support this position.

Linking the clinical director of cybersecurity to the CMIO seems like a natural connection. However, CMIOs historically have not focused on this area. Vi Shaffer of Gartner, Inc., conducted voluntary surveys of the members of the Association of Medical Directors of Information Systems over the course of several years. One survey question asked, "What three words come to mind when describing the CMIO role in 2018?" During a presentation, Shaffer listed the survey results in the form of a "word cloud," and "cybersecurity" was not anywhere near the CMIOs' top priority.[26]

Examples of Clinicians as Partners in Cybersecurity

Recently, the University of California, San Diego (UCSD) reported that it had appointed an emergency medicine physician as "medical director of cybersecurity." This individual had graduated from the university's informatics program. In its announcement, UCSD leadership wrote, "In his role, the medical director of cybersecurity will work closely with the security team in the Information Services (IS) department, to continue defending the enterprise from cyberthreats. He will also contribute to future enterprise cybersecurity strategy and liaise with the clinical department leadership to strengthen the organization's cybersecurity posture."[27]

Several years prior to this, the CMIO of a large southwestern medical organization appointed a cardiologist as "medical director of security." The physician had complained about workflow challenges introduced at seemingly random times in the organization. He was invited to become a key member of the organization's security and privacy committee, which developed policies in these areas. The committee met monthly to review plans for security and privacy changes and to deal with specific issues. They also met ad hoc for emergencies.

Prior to adding the cardiologist to the committee, decisions from IT security seemed arbitrary and frequently were met with resistance because they affected STEEEP. After the formation of the committee and regular communication of its activities, clinicians understood that they had a physician representative trying to balance clinical and security needs. Importantly, they also had a person with whom they could communicate.

National Implications and Support

Cybersecurity is more than just a local issue. Healthcare is one of the nation's 16 critical infrastructures,[28] and cyber incidents can have national security implications. Cyber invaders cannot be repelled through individual or local efforts alone any more than a state's national guard can fight off an invasion by a foreign power. National programs need to be utilized to help hospitals and other clinical organizations understand the importance of partnering with their clinicians regarding cybersecurity and to help clinicians understand the importance and benefits of engaging on the topic. Similar to our rationale of the importance of clinical cybersecurity leadership and decision making on the local level, such programs should be established on the regional and national level and are of national importance (e.g., in the case of a cyberattack on our healthcare and public health infrastructure).[29]

Model governance and education tools, certification programs, and tools for measuring the effectiveness of clinician understanding and involvement need to be developed. Standard tools for measuring, managing, and reporting cyber weaknesses and their risk to patient safety and care delivery need to be provided.

Clinical directors of cybersecurity should have national support through professional, informatics, and cybersecurity associations, along with support from national government agencies (e.g., HHS, FDA, Department of Homeland Security) and other healthcare-focused cybersecurity organizations

(e.g., Association for Executives in Healthcare Information Security, Health Information Management Systems Society, Health Information Sharing and Analysis Center). The National Institutes of Health should recognize this as area of important research and fund it appropriately.

Conclusion

Cyberthreats are becoming more frequent and malicious, and financially or politically motivated adversaries are executing well-planned, skillful, and stealthy attacks. The healthcare industry's cyber capabilities must improve to avoid looming disaster.

Better cyber defenses are not merely a matter of better tools, processes, and education, and it can't be left solely to technical staff. As clinicians who care about STEEEP, we cannot sit by and hope that our security professionals will protect us in a way that gives appropriate consideration to the safety and effectiveness of care. Rather, we need to act now to become true partners in cybersecurity, by incorporating clinicians into the new cybersecurity paradigm, including developing a new specialty—the clinical director of cybersecurity.

This article proposes a path forward and discusses a number of scenarios and solutions. Safe and successful use of secure technology and responses to cybersecurity incidents require collaboration. It's not easy, but our future depends on learning how to do this.

Acknowledgments

The authors thank *BI&T's* anonymous peer reviewers and Christian Dameff, MD, for their constructive feedback that helped improve the article.

References

1. Davis J. 3 weeks after ransomware attack, all 400 UHS systems back online. https://healthitsecurity.com/news/3-weeks-after-ransomware-attack-all-400-uhs-systems-back-online. Accessed Dec. 3, 2020.
2. Davis J. 5 providers still in downtime, as Sky Lakes confirms Ryuk ransomware. https://healthitsecurity.com/news/5-providers-still-in-downtime-as-sky-lakes-confirms-ryuk-ransomware. Accessed Dec. 3, 2020.
3. Wirth A. Ransomware-linked death hits close to home. https://aamiblog.org/2020/09/25/axel-wirth-ransomware-linked-death-hits-close-to-home. Accessed Dec. 3, 2020.
4. Cybersecurity & Infrastructure Security Agency. Ransomware activity targeting the healthcare and public health sector. https://us-cert.cisa.gov/ncas/alerts/aa20-302a. Accessed Dec. 3, 2020.
5. Davis J. 50% of ransomware attacks lead to data exfiltration; payments hit $234K. https://healthitsecurity.com/news/50-of-ransomware-attacks-lead-to-data-exfiltration-payments-hit-234k. Accessed Dec. 3, 2020.
6. Warminsky J. Data breach at Finnish psychotherapy center takes a darker turn with extortion attempts. www.cyberscoop.com/finnish-psychotherapy-data-breach-vastaamo. Accessed Dec. 3, 2020.
7. Morgan S. Cybercrime to cost the world $10.5 trillion annually by 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. Accessed Dec. 3, 2020.
8. Morgan S. Healthcare Industry to spend $125 billion on cybersecurity from 2020 to 2025. https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025. Accessed Dec. 7, 2020.
9. Wirth A. Cyberinsights: it's complicated. *Biomed Instrum Technol.* 2020;54(4):298–301.
10. DataBreaches.net. TheDarkOverlord dumps 180,000 patients' records from 3 hacks. www.databreaches.net/thedarkoverlord-dumps-180000-patients-records-from-3-hacks. Accessed Dec. 3, 2020.
11. Johnson T. How The Dark Overlord is costing U.S. clinics big time with ransom demands. www.mcclatchydc.com/news/nation-world/national/national-security/article150678617.html. Accessed Dec. 3, 2020.
12. Thomas G. Defending your data from The Dark Overlord. www.idigitalhealth.com/news/defending-your-data-from-the-dark-overlord. Accessed Dec. 3, 2020.
13. Martinez A. Story behind the DDoS attack vs Boston Children Hospital. www.thethreatreport.com/story-behind-the-ddos-attack-vs-boston-children-hospital. Accessed Dec. 3, 2020.
14. Blake A. Flint hospital targeted by Anonymous, hit by hackers amid water crisis fallout. www.washingtontimes.com/news/2016/jan/22/

flint-hospital-targeted-by-anonymous-hit-by-hacker. Accessed Dec. 3, 2020.

15. Davis J. 5 more healthcare providers fall victim to ransomware attacks. https://healthitsecurity.com/news/5-more-healthcare-providers-fall-victim-to-ransomware-attacks. Accessed Dec. 3, 2020.

16. UK Department of Health & Social Care. Lessons learned review of the WannaCry ransomware cyber attack. www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber attack-cio-review.pdf. Accessed Dec. 7, 2020.

17. Robert P. NotPetya infection left Merck short of key HPV vaccine. https://securityledger.com/2017/10/notpetya-infection-left-merck-short-key-vaccine-gardasil. Accessed Dec. 3, 2020.

18. Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world. Accessed Dec. 3, 2020.

19. Rautmare C. 'Dark Overlord' hacker sentenced to 5-year prison term. www.bankinfosecurity.com/dark-overlord-hacker-sentenced-to-5-year-prison-term-a-15038. Accessed Dec. 3, 2020.

20. Jarrett M. Cybersecurity: a serious patient care concern. *JAMA*. 2017;318(14):1319-20.

21. American Medical Association, Accenture. Taking the physician's pulse. www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/medical-cybersecurity-findings.pdf. Accessed Dec. 3, 2020.

22. American Medical Association, WSJ Custom Studios. Why doctors need more help with cybersecurity. https://partners.wsj.com/ama/charting-change/doctors-need-help-cybersecurity. Accessed Dec. 3, 2020.

23. Rachal M. US needs cyber-savvy doctors as connected device use rises, FDA panel says. www.medtechdive.com/news/us-needs-cyber-savvy-doctors-as-connected-device-use-rises-fda-panel-says/562658. Accessed Dec. 3, 2020.

24. Mezher M. Abbott recalls 465,000 pacemakers for cybersecurity patch. www.raps.org/regulatory-focus%E2%84%A2/news-articles/2017/8/abbott-recalls-465,000-pacemakers-for-cybersecurity-patch. Accessed Dec. 7, 2020.

25. Weaver C. Patients put at risk by computer viruses. www.wsj.com/articles/SB10001424127887324188604578543162744943762. Accessed Dec. 7, 2020.

26. Shaffer V. 2018 AMDIS-Gartner 14th Annual CMIO Survey: key findings. http://amdis.org/wp-content/uploads/2018/07/2018-AMDIS-PCC-AMDIS-Gartner-Survey-Shaffer.pdf. Accessed Dec. 3, 2020.

27. Hagland M. First in U.S. healthcare: UC San Diego Health appoints a medical director of cybersecurity. www.hcinnovationgroup.com/cybersecurity/medical-device-security/article/21091447/first-in-us-healthcare-uc-san-diego-health-appoints-a-medical-director-of-cybersecurity. Accessed Dec. 7, 2020.

28. American Hospital Association. Cybersecurity and hospitals: four questions every hospital leader should ask in order to prepare for and manage cybersecurity risks. www.aha.org/system/files/2017-12/ahaprimer-cyberandhosp.pdf. Accessed Dec. 3, 2020.

29. MITRE Corporation. *Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook*. www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf. Accessed Dec. 3, 2020.