Cybersecurity

APPLYING HOLISTIC RISK TO TELEMEDICINE—DIFFERENT USES, DIFFERENT RISKS

October 17, 2017

Telemedicine: Post by Peter Sheingold and Catherine Barrett

What happens if an intensive care unit (ICU) doesn't have access to the expertise needed to address a patient in critical care? What if you want to communicate with your doctor but want to avoid the waiting room?

In the CyberPhysicalHuman world, telemedicine services allow doctors to treat you from anywhere. But holistic risks of safety, reliability, confidentiality, availability, and integrity could be exploited to harm you.

Comparing two telemedicine services—Tele-Intensive Care Unit (Tele-ICU) and Mobile Medical Applications (mobile apps)—illustrates that holistic risk in a CyberPhysicalHuman world is not "one size fits all." Like cyber enabled services and devices in many other industries, it changes based how specific services and devices will be used.

Prioritizing Holistic Risk for Tele-ICU Services

Tele-ICUs use networked technology to allow doctors and nurses at a patient's bedside in one location to virtually, and in real time, connect with specialists to exchange patient information, monitor patient status, and respond to patient needs in another location. [i]

How would a provider of Tele-ICU services prioritize holistic risk associated with Tele-ICU services?

As shown in Figure 1, they would most likely prioritize risks associated with safety (e.g., a provider is unable to adhere to the accepted medical standard of care), reliability (e.g., a patient is unable to receive consistent access to the correct medical services), availability (e.g., a patient or provider is unable to receive, or access,

Figure 1: Tele-ICU Holistic Risk

services when needed) and integrity (e.g., a system or data that is informing treatment decisions is incorrect or corrupted) over confidentiality (i.e., patient information is improperly disclosed).

Why? Safety, reliability, availability, and integrity pose risks individually and together that could result in physical harm, or death, to a patient in a Tele-ICU environment.

For example, if a cyber-attack results in a specialist in one location not being able to access a patient's electronic health record to review dosages and prescriptions (i.e., availability), then he/she would not be able to make an informed diagnosis and develop an informed treatment plan for the patient (i.e., safety). Similarly, if a cyber-attack on the Tele-ICU software platform results in inconsistent real-time transmission of correct patient vital signs (i.e., reliability) to the specialist, then the specialist would not be able provide timely expertise (i.e., availability). Finally, if a cyber-attack alters patient data such as treatment plans or dosages (i.e., integrity), then specialists would not be able to make an accurate, informed diagnosis and develop an informed treatment plan for the patient, or onsite providers might administer inappropriate or even harmful interventions (i.e., safety).

There are also very real confidentiality risks associated with a cyber-attack in a Tele-ICU environment. For example, an exfiltration of medical data from Tele-ICU systems (software, hardware) could result in identity theft or personal embarrassment, and may put health providers at legal risk for state and/or federal criminal and civil penalties. While these are all real consequences, they are not as serious as the physical harm and safety consequences associated with the other holistic risk elements.

Prioritizing Holistic Risk for Mobile Apps

Mobile apps offer a direct way to access medical care and communicate with a licensed doctor or therapist at any time of night or day, 365 days a year. Mobile apps can be used for a broad range of educational, diagnostic, and treatment purposes, and depending on their specific uses, may be subject to FDA regulation.

This blog series focuses on a narrow use of mobile apps as a platform to connect patients and licensed healthcare providers for basic medical care (e.g., diagnosing and treating colds, flu, upper respiratory infections, skin infections, and some behavioral health issues).

What happens if a cyber-attack targets the mobile app? As shown in Figure 2, the risk profile is not identical to a Tele-ICU. Providers would likely prioritize risks associated with safety and integrity over confidentiality, reliability, and availability.

For example, if a cyber-attack alters prescription data (i.e., integrity), then it is possible the prescription could be inaccurately written— for the incorrect medicine or the

incorrect dosage or both. Thus, it is possible the patient could be given an inaccurate drug, dosage of drug or both, resulting in potential patient harm (i.e., safety).

Confidentiality will also be important.

A data breach of personally identifiable information (PII) or protected health information (PHI) held by the mobile app provider could result in criminal and/or civil penalties under federal and/or state law for exposure of protected medical information.
[ii]
In addition, patients using the mobile app services could be at risk for identity theft and/or medical fraud if hackers exfiltrate PII. And, the mobile app provider would likely suffer reputational harm for failing to adequately protect PII and their patients using the online doctor's office.

If, however, the mobile app software platform is attacked and access to the online site is disrupted or temporarily unavailable (i.e., reliability, availability), the patient is inconvenienced, but there is no risk of bodily harm.

Figure 2: Tele-App Holistic Risk

As these two use cases demonstrate, depending on how different devices or services will be used, they present different holistic risk profiles. A provider of Tele-ICU services would likely prioritize risks associated with safety, reliability, availability, and integrity over confidentiality. In contrast, a provider of mobile app services would likely prioritize risks associated with safety, integrity, and confidentiality over reliability and availability.

While you may not be in the healthcare industry, we hope this risk comparison provides a conceptual example that is applicable in your organization. Learn who has the obligation and opportunity to manage these risks.

Telemedicine: A Three-Part Series about Technology Convergence and Holistic Risk
Post #1: The Telemedicine and Holistic Risk Back Story
Post #3: Managing Holistic Risk in Telemedicine: A Stakeholder Perspective

About Catherine Barrett

Catherine Barrett is a cyber policy principal with MITRE and co-author of *What Is...Telemedicine?*, a health law primer on telemedicine published by the American Bar Association. She received her JD and MBA from the American University

Washington College of Law and Kogod School of Business, respectively. She may be reached here.

About Peter Sheingold

Peter Sheingold is a Principal who has worked on a range of cybersecurity challenges that lie at the intersection of strategy, policy, organization, operations, and technology. For questions or to comment, Peter Sheingold can be contacted here.

[i] Sajeesh Kumar, PhD; Shezana Merchant, MD; and Rebecca Reynolds, EdD, RHIA, "Tele-ICU: Efficacy and Cost-Effectiveness of Remotely Managing Critical Care," *Perspectives in Health Information Management* (Spring 2013), page 1 of 13, http://perspectives.ahima.org/tele-icu-efficacy-and-cost-effectiveness-of-remotely-managing-critical-care/. Tele-ICUs generally offer three clinical models of care: (1) continuous care model; (2) scheduled care model; and (3) responsive care model. In this series of blog posts we are using a continuous care model where Tele-ICU services provide continuous monitoring of the patient without interruption for a period of time. *See* American Telemedicine Association, "Guidelines for Telemedicine Operations," May 2014, http://www.learnicu.org/SiteCollectionDocuments/Guidelines-ATA-TeleICU.pdf.

[ii] PII is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. *See* http://privacyoffice.med.miami.edu/faq/privacy-faqs/what-is-personally-identifiable-information-pii

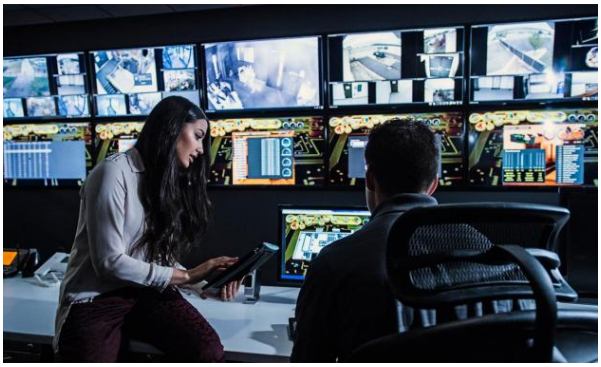
Related Technical Papers

Eight Recommendations for Congress to Improve Federal Cybersecurity

Breaking the Ransomware Cyc National Policy Options

SEE ALL TECHNICAL PAPERS

Related Projects



Pioneering New Ways to Protect Our Nation

Paving the Way for Automated Dı Systems

SEE ALL PROJECTS