Cybersecurity

# MANAGING HOLISTIC RISK IN TELEMEDICINE: A STAKEHOLDER PERSPECTIVE

October 17, 2017

Telemedicine: Post by Peter Sheingold and Catherine Barrett

A cyber-attack on a Tele-ICU could physically harm a patient; a cyber-attack on a mobile app could expose sensitive patient data. Who has the obligation and opportunity to manage these risks?

In the healthcare ecosystem, like many other industries, there no single stakeholder with either the complete obligation or opportunity to manage all risks. Some of the stakeholders most directly impacted by a potential cyber-attack in a Tele-ICU and/or mobile app environment are patients, payers, and providers.

Depending on the telemedicine service—Tele-ICU or mobile app—these stakeholders will likely have different obligations in law and policy and technical and operational opportunities to mitigate the different elements of holistic risk.

- **Patients:** Individuals who receive or use Tele-ICU or mobile app services
- **Payers**: Private insurance companies or government agencies that pay providers for Tele-ICU or mobile app services
- **Direct Service Providers (DSPs)**
  - **Tele-ICU:** Receiving hospitals with ICU patients.
  - **Mobile App:** Healthcare providers such as doctors or nurses providing medical care to the consumer/patient via a networked application
- **Third-Party Service Providers (TPSP)**
  - **Tele-ICU**: The Tele-ICU TPSP is a business that typically integrates a proprietary software platform with hardware (e.g., audio and video capabilities) and independently contracts critical care specialists (e.g., doctors, nurses) to provide ICU services to the ICU hospital staff at the patient's bedside. Hiring critical care specialists as independent contractors may limit the exposure of the TPSP to some potential claims of liability for personal injury and/or negligence.[i]
  - **Mobile App**: The mobile app TPSP is a business that typically consists of a proprietary software platform and independently contracted providers (e.g., doctors, nurses, psychotherapists) who treat minor illnesses (colds, flu,

etc.). If necessary, doctors and/or nurse practitioners write and send prescriptions to the patient's pharmacy of choice.

From a legal and policy perspective, individual stakeholder group obligations are driven by a variety of laws—contract law, medical malpractice law, data privacy and security law and tort law—as well as federal laws and policies set by state medical boards. For example, medical boards in each of the 50 states define the criteria to license doctors and establish the legal minimum standards and duty of care doctors owe to patients.

A duty of care refers to the obligation a doctor owes a patient to take reasonable care to avoid foreseeable patient harm and extends to hospitals to maintain a safe environment and adequate equipment and facilities. Doctors who fail to meet the standards of care to their patients risk liability associated with medical negligence. Differences in state laws and policies means that there isn't a single legal standard of care that all stakeholders must meet. Determining what level of obligation an individual stakeholder may have to address cybersecurity risks associated with telemedicine requires a state-by-state legal and regulatory analysis.

*Tele-ICU*

**Patient Obligation/Opportunity to Manage Tele-ICU Risk**

In a Tele-ICU setting, patients are critically ill and cannot perform due diligence to mitigate potential cybersecurity risks.

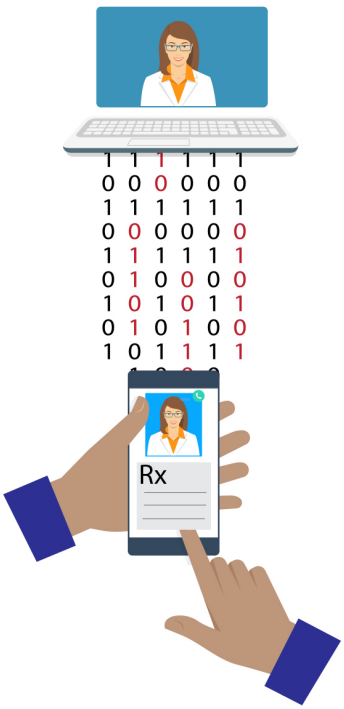
**Payer and Provider Obligation to Manage Tele-ICU Risk**

Risks associated with safety, reliability, integrity, and availability are more serious, as they could potentially cause physical harm or death to patients, and could result in negligence lawsuits against providers.[ii] However, there is not a consistent and clear legal/policy obligation across all 50 states to address these risks. In the case of Third Party and Direct Providers, the obligation would be derived from the duty of care that providers owe to patients, based on the specific state-by-state legal standards of care.

Obligations to address risks associated with confidentiality, while comparatively less serious, are more consistent and clear. Payers and providers have obligations to address confidentiality risks associated with protecting patient's personally identifiable information. These obligations emanate from federal HIPPA law and regulations, and state data privacy and/or security laws.[iii] In addition, they could face regulatory scrutiny from the Federal Trade Commission (FTC) for "for unfair or deceptive practices that endanger the personal data of consumers,"[iv] based on inadequate data security.

### Payer and Provider Opportunities to Manage Tele-ICU Risk

Payers, Third Party, and Direct Providers have a range of technical and operational opportunities to manage risks associated with Tele-ICU. These include, but are not limited to, applying and adopting a range of cybersecurity controls (e.g., firewalls, system patching, encryption, access controls); ensuring that contracts with third-party providers include security requirements; and obtaining cyber-liability insurance policies that go beyond data or privacy breach protections.[v],[vi],[vii] However, and even more fundamental, is a focus on resilience. Mitigating risks to devices such as those used in Tele-ICUs, which could put human safety at risk, requires a recognition that an organization's vital mission and business functions must be able to continue despite adversary attacks. Depending on the specific stakeholder, certain resilience techniques may be more suitable (e.g., network segmentation, redundancy, and privilege restriction).




*Mobile-App*

### Patient Obligation/Opportunity to Manage Mobile App Risk

While patients do not have a legal/policy obligation to mitigate risks, patients in a mobile app environment have opportunities to manage, but not eliminate, risks to personal safety and data confidentiality by practicing "good cyber hygiene" on their personal devices that use a mobile app. For example: downloading, launching, and regularly updating anti-virus software; downloading and updating operating system software; using complex passwords; and avoiding the practice of clicking on links embedded in emails (possible phishing attacks).

### Payer and Provider Obligation to Manage Mobile App Risk

These stakeholders are obligated to address risks associated with data confidentiality that derive from federal and state laws. Addressing risks associated with safety, reliability, integrity, and availability today is less clear and consistent across all 50 states, and, in the case of providers, would be largely driven by state-by-state duty of care standards.

### Opportunities to Mitigate Mobile App Risks

As reliability and availability risks associated with mobile apps are more likely to result in patient inconvenience, rather than patient harm, enabling continued mission performance through all attack is less vital than in a Tele-ICU environment. However, as mobile apps are used to address core mission imperatives (i.e., deliver medical care to patients), cyber breaches would represent a "mission breach" that could damage

public trust and reputation. Thus, applying resilience techniques could be useful in a mobile app environment.

**Wrapping It Up**

While we focused on a particular sector—health care—and a specific category of medical service delivery—telemedicine—the underlying concepts we explored are intended to be broadly applicable. Across many sectors and industries, converged CyberPhysicalHuman technologies are being used to improve service delivery, and in so doing pose a broad array of risks that could cause physical harm to people and put organizational missions in jeopardy. However, the holistic risk profile will likely differ on a service-by-service or device-by-device basis.

In many cases, no single stakeholder will likely have the full obligation and opportunity to manage these risks. And, the legal and policy landscape may not be fully caught up to the technical capabilities that are now being deployed. Regardless of the sector or industry you work in, we hope the telemedicine story has given you some ideas about how you can approach these challenges.

**Telemedicine: A Three-Part Series about Technology Convergence and Holistic Risk**
Post #1: The Telemedicine and Holistic Risk Back Story
Post #2: Applying Risk to Telemedicine – Different Uses, Different Risks

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] Employers who hire employees rather than independent contractors are exposed to potential claims of liability from the actions of their employees. Under the rule of respondent superior, an injured party will seek to recover from the person or persons directly responsible for the injury as well as the person's employer, recognizing that both the person and the person's employer may have acted negligently, resulting in

injury to the party. "Respondeat superior is an extension of the principle of vicarious liability that holds an employer responsible for the conduct of an employee" *See* Black's Law Dictionary, http://thelawdictionary.org/article/three-conditions-required-respondeat-superior/.

[ii] Negligence is proved if all parts of a three-part test are satisfied: (1) the hospital owes a duty of care to patients; (2) the duty was breached; and (3) the patient suffered harm as a direct result of the breach. Specifically, under the theory of corporate negligence, hospitals have a "'nondelegable duty to provide reasonable and safe healthcare to its patients and that direct liability can arise for negligent care." Sal Fiscina, *Liability of Health Care Entities for Negligent Care,* Legal Medicine*,* 7th Edition, Chapter 36, June 12, 2007, https://books.google.com/books?id=8gajBQAAQBAJ&pg=PR6&lpg=PR6&dq=Sal+Fiscina+Liability+of+Health+Care+Entities+

[iii] Payers, including private health insurance companies and government programs such as Medicare and Medicaid, and clearinghouses, are subject to data privacy and security laws outlined under the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is designed, in part, to protect PII and keep this information confidential, allowing only authorized parties to have access to PII. *See* https://www.cms.gov/regulations-and-guidance/administrative-simplification/hipaa-aca/areyouacoveredentity.html.

[iv] William R. Denny, "Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act," American Bar Association Business Law Today, 2016, https://www.americanbar.org/publications/blt/2016/06/cyber_center_denny.html. The Federal Trade Commission (FTC) has not provided bright line rules defining what constitutes "reasonable and necessary measures" for implementing a cybersecurity program, but it has provided guidance. The FTC website publishes guidelines, tips, and advice for businesses, and past complaints and consent orders. *See* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security. *See also* Jeff Kosseff, *Cybersecurity Law* 6, (1st ed. 2017). *See FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

[v] American Telemedicine Association, "Guidelines for Telemedicine Operations," May 2014, http://www.learnicu.org/SiteCollectionDocuments/Guidelines-ATA-TeleICU.pdf. Systems should comply with the Federal Information Processing Standard, the U.S. government security standard used to accredit encryption standards of software and lists encryption such as Advanced Encryption Standard.

[vi] Examples of redundant technologies may include N+1 redundancy, geographic dispersed infrastructure, fast failover, failure notifications/alerts, and/or documented "on call" procedures during planned or unplanned Tele-ICU downtime. American Telemedicine Association, "Guidelines for Telemedicine Operations," May 2014, http://www.learnicu.org/SiteCollectionDocuments/Guidelines-ATA-TeleICU.pdf.

[vii] Some of these risk mitigation measures are summarized from The Advisory Board Company, "Healthcare Law Round Table: General Counsel Agenda," June 2014, https://www.advisory.com/-/media/Advisory-com/Research/HCLR/White-Papers/GC-Agenda-Q2-2014-2.pdf.

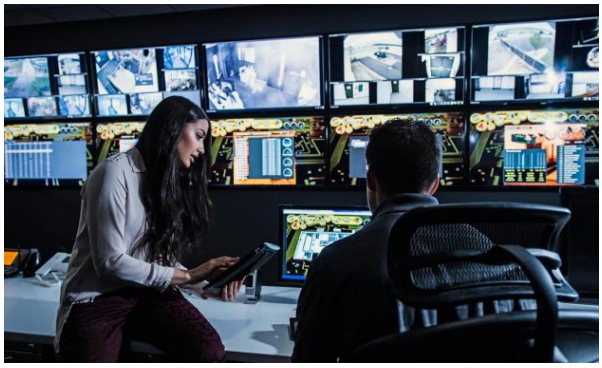
## Related Technical Papers

**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 Dr Systems

SEE ALL PROJECTS