Articles + Publications | June 7, 2024

Checking the Pulse: An Approach to Telehealth Privacy and Cybersecurity Due Diligence

WRITTEN BY

Brent T. Hoard | Erin S. Whaley | Emma E. Trivax

In the rapidly evolving landscape of health care, the surge in telehealth has been nothing short of revolutionary. This digital transformation, while offering unprecedented access to health care services, also introduces a complex web of privacy and cybersecurity challenges. As telehealth continues to expand, understanding and mitigating these risks becomes crucial for any entity considering financing or acquisition in this space. While this article focuses on privacy and cybersecurity, other health care compliance issues, such as the corporate practice of medicine, proper licensing, state telehealth regulations, patient consents, and Stark/Anti-Kickback Statute compliance, are key considerations in any prospective telehealth deal.

Privacy and cyber preparedness, exposure to breaches, ransomware, and data leaks, and the rise in Office for Civil Rights (OCR) fines and class action lawsuits are impacting deal diligence and even valuations in health care and telehealth. In this article, we present an approach to pre-diligence and diligence that is designed to identify potential risks and efficiently assess the scope and maturity of the privacy and cyber programs at a telehealth target. If you are preparing to finance or sell your telehealth business, reverse the approach to anticipate and prepare for likely requests from savvy financing partners and buyers.

Step 1: Use Pre-Diligence Review to Set the Stage for Diligence

Before the Virtual Data Room (VDR) is open or even pre-Letter-of-Intent (LOI), you can establish initial expectations and scoping for privacy and cyber diligence.

1. Consider the Potential Regulatory Environment

Identify regulations that you think apply, or may apply, to the target. Health Insurance Portability and Accountability Act (HIPAA) is a starting point, given that health information is involved. Even if the target is not subject to HIPAA, health information is, by its nature, “sensitive” and may be subject to regulation under other state-specific privacy laws (*e.g.*, the California Consumer Privacy Act or Washington’s My Health My Data law), the Federal Trade Commission’s (FTC) Health Breach Notification Rule, or international privacy laws like the General Data Protection Regulation. Also, consider whether any telehealth waivers that were enacted during the COVID-19 pandemic under Section 1135 of the Social Security Act are still applicable to the target, or if the target is still following an expired waiver.

2. Identify Potential Risks

While each target is unique, common “red flags” for privacy and cyber include breaches, regulator actions or inquiries, complaints about privacy and/or security practices, and data use limitations or restrictions. Additionally, consider risks specific to telehealth such as transmission security, data storage and retention, encryption, penetration testing and vulnerability scanning, access controls, asset management, and third-party vendors.

3. Conduct a Pre-Diligence Review

Conduct a pre-diligence review at an early stage in the transaction lifecycle, even before a term sheet is signed. It is intended to provide a high-level overview without dedicating substantial resources. This review can help identify potential red flags or other material issues and, along with the regulatory scope and risk profile, inform the scope of more detailed due diligence activities to follow. Some things to incorporate into your review may include the following:

- Review online breach repositories (OCR and certain U.S. states).
- Use a tool to identify active tracking technologies on the target’s website (especially important given the OCR’s recent focus on AdTech).
- Review the target’s privacy policy to determine compatibility of data rights (*e.g.*, do current use cases align with preferred post-close uses), whether there are restrictions or gratuitous promises to address (*e.g.*, opt-in or opt-out consent is required for the transaction), and whether secondary uses are permitted (*e.g.*, de-identification; data can be used for service improvement or analytics).
- Review the target’s website for public representations about its data practices (*e.g.*, “We’re HIPAA certified!), adherence to industry frameworks (*e.g.*, HITRUST, NIST), or use of potentially higher-risk technologies such as AI.

Establishing this baseline understanding of the telehealth target, sets the stage for diligence in Step 2.

Step 2: Prepare and Organize to Execute Successful Diligence

Use the information gathered during pre-diligence to develop your due diligence request list (DDRL) and a framework for organizing diligence issues.

1. Considerations for the DDRL

In addition to standard diligence requests (*e.g.*, compliance program policies and procedures), include customized requests based on the pre-diligence review. At a high-level, you will want to request program materials and responses to answer key questions such as:

- What telehealth platform is in use at the target?
- Does the target provide notices to patients about their participation in a telehealth arrangement?

- How is patient data transmitted and stored in the telehealth platform?
- What safeguards and controls are in place for the telehealth platform and any health data that might be stored elsewhere in the target's environment?
- Has the target conducted a HIPAA Security Rule risk analysis? If so, what risks did the target identify and how are those risk mitigated?
- How does the target manage vendor risk within its telehealth ecosystem?
- Has the telehealth target experienced any breaches, litigation, or complaints or is it subject to a regulator inquiry (*e.g.*, the OCR or FTC)?

2. Use a Framework to Organize Diligence and Analysis

Consider developing and using a framework to organize common privacy and security diligence issues into key categories and subcategories to guide, simplify, and promote consistency in the due diligence process. A framework can be used as a roadmap for issue-spotting in the diligence process and to organize due diligence reporting and integration/remediation planning. At a high level, common diligence issues fall into five key categories:

1. Privacy Program and Compliance Issues
2. Data Rights and Limitations
3. Information Security
4. Breaches and Incidents
5. Enforcements and Legal Actions

Step 3: Identify Key Remediation Action Items and Timing to Address Risks/Issues

During the diligence process, consider how you will address any identified compliance risks or business issues and plan for the integration of the target into your business. While some priority action items must be addressed pre-close, most privacy and cybersecurity issues will be included in a post-close integration plan.

- **Pre-close action items.** These are actions that must be taken before the deal closes or conditions that must be addressed before or at closing. Examples of these pre-close action items include obtaining consent to the transfer of personal information in a transaction or remediation of a material security vulnerability.
- **Post-close remediation.** Decide whether the target company's privacy and cyber compliance programs will be

integrated into your business and programs, or whether it will operate independently. Develop a roadmap for integration to help inform the decision-making process. A roadmap will help you assess the timing, level of effort, resources, and cost associated with the integration.

Conclusion

A strategic and intentional diligence process will enable investors and buyers to efficiently and effectively navigate the complexities of a telehealth deal, ensuring a thorough assessment of privacy and cybersecurity risks, and laying the groundwork for successful post-close integration and remediation.

The Troutman Pepper team is ready to assist with your next deal or with more general telehealth privacy, cybersecurity, and compliance needs. Please contact Brent Hoard at brent.hoard@troutman.com, Erin Whaley at erin.whaley@troutman.com, or Emma Trivax at emma.trivax@troutman.com for more information.

RELATED INDUSTRIES + PRACTICES

- Corporate
- Data + Privacy
- Health Care + Life Sciences
- Health Care Regulatory
- Privacy + Cyber