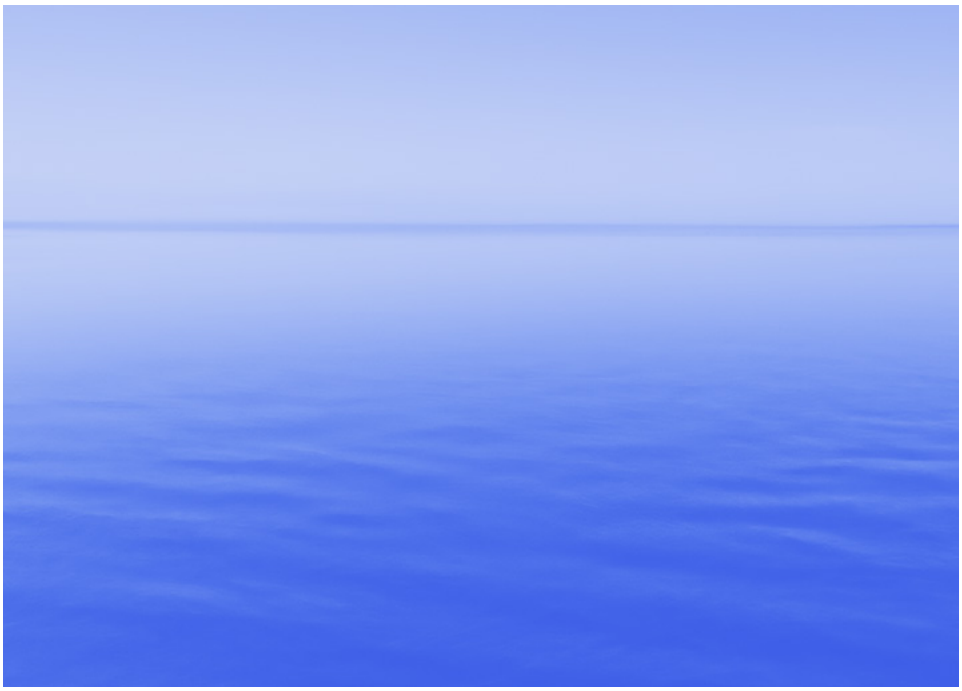
Clearwater

Whitepaper

Let the Buyer Beware: The Need for HIPAA Risk Analysis in Healthcare M&A Transactions

Table of Contents



Introduction

Healthcare mergers, acquisitions, and joint venture partnerships have surged in recent years, driven by increasing opportunities to innovate, improve quality, and reduce costs. The advancement of new business models and consolidated platforms also have played an important part in the surge.

Over the last decade, strategic acquirers and private equity investors have integrated thousands of HIPAA covered entities and business associates into their portfolios. Through these experiences, they have become much better educated on the regulatory and reputational risk counterparties bring as a result of a privacy or security breach.

An all-time high 40 million healthcare records were breached in 2019.[1] In 2020, ransomware attacks against healthcare organizations have grown to the highest levels of all time.[2] Reading about these attacks in the daily headlines, investors often think "that won't happen to us" – until it does. Any investor who has lived through a nightmare breach scenario within its portfolio is all too familiar with the associated costs, business disruption, and potential regulatory scrutiny.

Past breaches may cause future liabilities

In addition to future cyberattacks and privacy breaches, buyers need to be concerned about liabilities they may be assuming as a result of the seller's non-compliance with HIPAA or failure to exercise the required duty of care in cybersecurity practices. It is not uncommon that breaches go undetected and unreported for months or even years, and thus they may not be identified in the diligence process.

While the seller will typically be responsible for a breach prior to close, determining and proving when a breach first occurred is often not straightforward, even with the support of expensive forensic experts. If the breach was ongoing and unidentified for some time after the purchase, it becomes an even more complicated affair. Additionally, federal and state regulatory actions and civil lawsuits typically follow for years after a breach, with

1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2 https://securityboulevard.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/

the buyer left managing an expensive and distracting situation. Failures of the past may weigh heavily on the organization's future growth trajectory.

> An all-time high 40 million healthcare records were breached in 2019.1 In 2020, ransomware attacks against healthcare organizations have grown to the highest levels of all time.[3]

Organizations that enter into joint ventures, make minority investments, or establish business partnerships also should take note of potential privacy and security liabilities and business ramifications that may occur from a counterparty's failure to comply with HIPAA or from its lack of due care in cyber risk management. Companies that partner with organizations that are responsible for safeguarding protected health information (PHI) should assess and limit their exposures in the event the other party fails to implement reasonable and appropriate security and privacy practices.

Review the counterparty's risk analysis as part of due diligence

For many years, HIPAA compliance and cybersecurity were only worthy of cursory levels of diligence in healthcare transactions. However, today we are finding that investors (in particular, private equity) and their attorneys are devoting more time and resources to this area. A preventable breach associated with HIPAA failures could be a non-starter for future acquirers and therefore might significantly reduce the value of the company at a future exit. As such, investors now have a stronger appetite to invest in diligence at the same levels they are accustomed to with other traditional categories such as financial, insurance, and IP.

Comprehensive HIPAA compliance and cybersecurity diligence must include a thorough review of the organization's security risk analysis. It must determine whether the risk analysis is up to date and if it complies with the **Office for Civil Rights' (OCR's)[4] Guidance on Risk Analysis Requirements under the HIPAA Security Rule**[5]. Demonstration of an accurate and thorough risk analysis is critical for several reasons:

3 OCR is the HIPAA enforcement arm of the U.S. Department of Health and Human Services.

4 https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

5 Clearwater proprietary database sourced from U.S. Department of Health and Human Services Office for Civil Rights Breach Portal and analysis of publicly announced civil money penalties and settlements

1. During an OCR investigation of a breach, one of the first things the assigned investigator will ask to review is the organization's risk analysis. A failure to conduct an enterprise-wide risk analysis of all of the organization's information assets according to the OCR Guidance, is the most common deficiency resulting in a civil money penalty or settlement. Failure to perform an adequate risk analysis is cited in 91% of these cases. Recent OCR enforcement actions support that its focus on compliance with the risk analysis requirement is not going away.[6]

2. As can be inferred from the above, what most healthcare organizations call a risk analysis does not meet OCR's standards. This is true even for larger organizations, which are more complex, and for whom the bar is set even higher. For more information on what is required in risk analysis, read Clearwater's blog on Performing an OCR-Quality® Risk Analysis or view our on-demand webinar on the subject.

3. A risk analysis is the only method by which the organization – and the acquirer – can truly know what actual cybersecurity risks exist for that particular organization. A risk analysis is not simply completing a controls checklist. Rather, it evaluates the specific vulnerabilities and threats to the organization's information systems and evaluates the controls in place and how well they mitigate risks. By reviewing the risk analysis, the buyer can understand what risks exist and at what level, and determine whether, based on its risk tolerance level, it will need to reduce those risks further. The buyer can work with its diligence consultant to estimate the cost and level of effort involved to reduce these risks, and therefore have better visibility into how much capital investment in the security program is required. As a result, it will have a better sense of the true acquisition cost of the target.

Does the risk analysis meet regulatory standards?

A risk analysis must meet OCR's definition and standards to be of any value. Make sure that (a) the review of the risk analysis receives particular attention in the compliance and cybersecurity due diligence process, and (b) whomever reviews the risk analysis is an expert in this area. A generalist cybersecurity firm, accounting firm, or other non-HIPAA Security Rule expert, will often not have the expertise required to make this determination.

6 https://www.lexology.com/library/detail.aspx?g=f473767f-e585-47d3-b2b9-2b85f25311a1

Ultimately, you should seek advice from your attorney when it comes to risk analysis diligence along with the broader HIPAA diligence process. Many healthcare transaction attorneys will ask one of their healthcare and privacy security partners to assist in this area or leverage a third-party healthcare cybersecurity consultant to perform the detailed review and produce a findings and observations report.

Include satisfaction of 45 CFR § 164.308(a)(1)(ii)(A)) in seller representations and warranties

Requiring representations and warranties related to HIPAA compliance along with other regulatory requirements may not be a new concept. What is new, is an emerging trend to specifically include representations of compliance with 45 CFR § 164.308(a)(1)(ii)(A)) of the HIPAA Security Rule – i.e. performance of a risk analysis. We would go further and suggest that the representations should include specifying that the risk analysis complies with the OCR guidance document previously referenced. Why is this so important? Attesting that the organization complies with HIPAA is broad, vague, and open to interpretation. Consider this: It is highly likely that many organizations that paid substantial fines thought they had performed a risk analysis correctly but did not. With risk analysis failure leading the reasons for regulatory enforcement, calling out that it must have been done following OCR guidance may provide more protection for the buyer or third-party partner.

Consult with your attorney as to whether you should require specific representations and warranties from the seller or partner related to their performance of a security risk analysis, which meets OCR standards as stated in its guidance. Ask your attorney how you can seek recourse from the seller in the case that you incur future damages resulting from regulatory actions or lawsuits that occur as a result of a risk analysis failure.

Addressing lack of, or inadequate, risk analysis

It is quite common to discover through your diligence that the target or partner has not performed an adequate security risk analysis that meets OCR's standards. Typical failures of risk analysis include (1) it has not been performed recently, (2) it does not include all of the organization's information assets used to create, receive, maintain or transmit ePHI, or (3) it does address reasonably anticipated threats and vulnerabilities. Additionally, the organization may have failed to respond to the high and critical risks that emerged from the analysis (known as the risk management plan).

As already discussed, failure to perform a risk analysis creates a risk of a potentially large liability for the company or partnership. In this case, there are several approaches you may take to reduce risk:

1. **Require that a risk analysis be performed by the seller (or in case of a joint venture, the partner) as a closing condition**. In our opinion, this is the optimal approach from a risk perspective; however, at the same time, one will not want it to delay the transaction. The ability to accomplish this quickly will largely be dependent on the scope of the risk analysis, the availability of the target's resources, and the capability of the assessor to move quickly. Aided by Clearwater's IRM|Analysis® software, our consultants have completed a risk analysis in less than 30 days. A typical practice would be to create the follow-up risk management plan post-closing.

2. **Require a risk analysis as a Post-Closing Covenant.** This might be a common and adequate approach in partnership agreements, minority investments, or other transactions where the seller or partner maintains control of the organization. This may also be a more practical approach to take when timing and resources are less flexible, and when other areas of HIPAA and cybersecurity diligence provide reasonable levels of comfort that the organization has strong controls in place but has not yet gone through the process of assessing them against risks that are relevant for its organization.

Consider this:

It is highly likely that many organizations that paid substantial fines thought they had performed a risk analysis correctly but did not.

3. **Buyer performs risk analysis post-closing.** In this case, the buyer is acquiring control of the company, and it can opt to perform the risk analysis after closing and should do so as soon as possible. The buyer must be comfortable with accepting the regulatory risk and the fact that until such time that it performs the risk analysis, it will not truly know the potential risks to the confidentially, integrity, and availability of patient data and the organization's information systems. Performing an OCR-quality analysis carries a material cost. The buyer may wish to seek a reduction in the purchase price or request other compensation. Note that there may be additional costs associated with responding to high or critical risks, but those won't be known until after the risk analysis is complete – a further argument for performing the risk analysis before closing.

Reps and warranties insurance trend: OCR-Quality® risk analysis required to underwrite claims due to HIPAA violations

The highly complex regulatory environment in healthcare, along with growing concerns about patient privacy and safety, result in a large number of potential future liabilities for which neither party wants to be responsible. As a result, negotiation over reps and warranties can be one of the most arduous and lengthy parts of the deal-making process. Reps and warranties insurance can solve this issue by protecting buyers from future liabilities. The use of this insurance has become increasingly more common in healthcare transactions with private equity firms. We have noticed several trends emerging with regard to reps and warranties insurance:

1. **Underwriters are requiring more comprehensive HIPAA and cybersecurity diligence.** Insurers are expecting that the buyer is using a qualified expert to perform an extensive amount of HIPAA diligence as part of its overall diligence efforts.

2. **Risk analysis specifically required to avoid exclusions**. Some insurers are going as far as to specifically require that a HIPAA Risk Analysis is performed prior to underwriting liabilities related to HIPAA compliance.

3. **Underwriters are relying on the risk analysis as a key input in determining coverage.** In addition to ensuring the risk analysis has not only been completed but also performed correctly, the insurer wants to know what high and critical risks exist, and may rely on them to justify further exclusions or limits to the coverage.

In summary

While the COVID-19 pandemic has slowed the pace of healthcare mergers and acquisitions temporarily, the trend is expected to resume and likely accelerate as business conditions normalize7. Fueled by the increase in cyberattacks, and damages incurred with their portfolio companies and joint ventures, investors can be expected to place increased emphasis on the execution of strong diligence of HIPAA compliance and cybersecurity practices as new deals develop. Risk analysis should take center stage as one of the most important components of compliance with the HIPAA Security Rule. In the case that the target or partner has not performed a risk analysis that meets regulatory standards, it should take action to solve for the deficiency by performing the risk analysis as soon as possible. Risk analysis reps and warranties can help protect buyers from counterparty failures, as can reps and warranties insurance. Knowledgeable underwriters will often require the insured party attests that it has not only complied with HIPAA, but that it also has performed an OCR-Quality Risk Analysis.

In developing your approach and strategy, always consult with your legal counsel. They can help you identify partners to conduct the HIPAA compliance and cybersecurity diligence, and if necessary, perform a risk analysis on a timeline that enables to achieve your transaction objectives.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact