GV LAW

HIPAA & DATA PRIVACY IN MEDICAL M&A: A HIDDEN LANDMINE

GV LAW INSIGHTS

Transactional activity in the healthcare sector continues to accelerate, particularly across specialties such as dermatology, dental, medspa, behavioral health, and outpatient surgical practices. As buyers, MSOs, and private equity platforms compete for assets, one issue consistently disrupts transactions, prolongs diligence, and exposes both parties to regulatory risk: the handling of protected health information ("PHI") under HIPAA.

While financial and operational metrics tend to receive the most immediate attention in healthcare acquisitions, data privacy compliance often becomes the most significant source of liability. Many parties assume that PHI can be accessed, shared, or migrated freely during the course of a deal. In reality, HIPAA imposes strict limitations on what information may be disclosed, under what conditions, and to whom. Failing to observe these limitations can trigger enforcement risk, require breach notifications, or materially alter the terms of a transaction.

A recurring issue arises when buyers attempt to conduct diligence on clinical operations. Sellers frequently allow broad access to electronic health record ("EHR") systems or provide spreadsheets that contain identifiable patient information, believing such disclosures are routine features of a sale process. HIPAA allows diligence access only under narrowly defined circumstances, and even then, the information provided often must be de-identified or subject to specific contractual protections. Inappropriate disclosure during diligence, whether intentional or inadvertent, can constitute a violation even if the transaction never closes.

EHR systems themselves present additional complications. Many practices utilize third-party platforms without maintaining updated Business Associate Agreements, leaving years of PHI storage in a legally uncertain position. Audit logs may be incomplete, user access may be poorly controlled, and historical migrations may have been executed without proper oversight. When a buyer acquires a practice, it may also inherit the consequences of prior noncompliance. This risk is amplified in multi-location practices or groups that have undergone several rounds of expansion or software transitions.

The post-closing integration period carries similar dangers. Transferring PHI between systems, onboarding staff, consolidating billing platforms, or merging patient portals can all become sources of inadvertent breaches if the transition occurs without a clearly defined, HIPAA-

compliant migration plan. Many breaches arise not from negligence but from the urgency and pace at which integration is attempted. A single misconfigured system or improperly shared database can create regulatory exposure for both parties immediately following closing.

These issues have direct transactional consequences. Buyers increasingly identify privacy concerns during diligence and respond by requesting extensive privacy representations, enhanced indemnification provisions, or escrow holdbacks to protect against undisclosed breaches. In certain cases, unresolved HIPAA deficiencies reduce purchase price, delay closing, or shift key economic terms. Sellers who enter the market without first assessing their privacy compliance posture often find themselves negotiating from a position of weakness.

For sellers, the most effective strategy is to undergo a privacy compliance review as part of pre-transaction preparation, ensuring that Notices of Privacy Practices, intake forms, Business Associate Agreements, and internal policies align with current regulatory requirements. For buyers, a disciplined privacy diligence process is essential, including a thorough review of EHR systems, vendor relationships, incident logs, data-handling procedures, and any history of complaints or investigations. Both parties benefit from clearly delineating when and how PHI may be accessed during diligence and from structuring the transaction with privacy obligations expressly defined.

GV LAW advises medical practices, MSOs, private equity sponsors, and multi-state operators on the privacy-related elements of healthcare transactions, including HIPAA diligence, PHI transfer protocols, MSA and PC-MSO structuring, EHR migration oversight, privacy representations and warranties, and post-closing compliance planning. Our approach integrates regulatory precision with practical deal execution, helping clients anticipate risk before it disrupts negotiations or undermines value.

Parties considering an acquisition or sale in the healthcare sector should treat HIPAA compliance as a central element of their transaction strategy. Early attention to data privacy issues reduces regulatory exposure, strengthens bargaining position, and facilitates a smoother path from diligence to closing.

For further guidance on HIPAA considerations in healthcare M&A, please contact GV LAW.