Navigating HIPAA and Cybersecurity in the Cloud

By Rick Hindmand, Attorney, McDonald Hopkins LLC

Physicians who use cloud-based for applications involving protected health information (PHI) face the task of satisfying the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements while effectively managing risks and serving the needs of their patients. This can be particularly challenging for functions relating to patient portals, online scheduling or electronic health records, where a data breach can go viral and affect thousands of individuals.

A cloud vendor that uses, creates or maintains PHI of its physician practice client acts in the role of the practice’s business associate, so the HIPAA Privacy and Security Rules would generally impose an obligation on both the cloud vendor and practice to enter into a written HIPAA business associate agreement (BAA).

While the Privacy and Security Rules mandate the inclusion of certain provisions in any BAA, these are the minimum elements, and should not be viewed as creating any one-size-fits-all standard for BAAs. In fact, it is typically in the interest of a covered entity (in this case, the practice) to include additional safeguards, such as requiring the cloud vendor to maintain specified levels of cybersecurity insurance and to provide indemnification for its noncompliance or data breach. Insurance and indemnification provisions can be a point of contention between the covered entity and business associate, due to the potential to shift potential costs between the parties. It is also common for covered entities to impose more stringent breach notification deadlines than set forth in the Breach Notification Rule and to require the business associate to mitigate any data breach by the business associate and assist in responding to the breach. Other possible provisions include notice and cure periods for termination, as well as restrictions on the ability of the business associate to use subcontractors, hold ePHI on offshore servers or create and use de-identified information.

Prior to entering into any new relationship with a cloud vendor and allowing access to PHI, it is crucial for a physician practice to review the underlying contract and the BAA together to understand the rights and obligations of the parties and then negotiate for adequate protection of its interests. In addition to the BAA issues noted above, some issues of particular significance include: (i) practice ownership of and access to all data, (ii) potential for the cloud vendor to hold the PHI hostage in the event of a contract dispute, (iii) encryption, (iv) regular backups, and (v) review the contract for any disclaimers of warranties or limitation of damages that may restrict indemnification or other remedies under the BAA and clarify that any such restrictions should not apply to remedies under the BAA.

Some cloud vendors present standard, bare bones BAAs that provide only limited protection for the interests of the covered entity. The physician practice should be sure to review and negotiate the proposed BAA or present its proposed BAA to the cloud vendor. Cloud vendors that view themselves as being in a strong negotiating position may be unwilling to revise their standard BAAs, in which case the practice may have limited room to negotiate, but should weigh the contractual deficiencies against the benefits of using the cloud vendor.

Existing cloud vendor and other service relationships should be reviewed periodically to identify all business associate relationships and determine whether a BAA is in place and, if so, the BAA and the underlying contract should be reviewed for HIPAA compliance as well as security and privacy protections. BAAs entered into prior to September 23, 2013 (the compliance date for the HIPAA Omnibus Rule), warrant close attention to confirm that all Omnibus Rule elements are satisfied. The Omnibus Rule included a grandfather clause that allowed some pre-January 23, 2013, BAAs to continue in use until September 22, 2014, but all BAAs are now required to comply with the BAA provisions of the Omnibus Rule.

A covered entity can suffer potentially ruinous costs in the event of noncompliance or a data breach, whether by the practice, its cloud vendor or other business associates. These costs can include fines and settlement payments, breach response costs (including fees of attorneys and IT consultants that can be particularly significant), and loss of goodwill after bad publicity. HIPAA-covered entities and business associates face increasing levels of scrutiny and exposure for claims that can be asserted by potential enforcers such as OCR, state attorneys general, the Federal Trade Commission (FTC) and plaintiffs’ attorneys. The upcoming HIPAA audits, which are expected to commence in early 2015, will subject covered entities and business associates to additional scrutiny.

A 2012 settlement by a small physician practice in Arizona (Phoenix Cardiac Surgery) illustrates some of the potential dangers of online patient scheduling systems. The practice agreed to pay $100,000 and take corrective action after patient appointments were posted on a publicly accessible Internet-based calendar. In that case, the practice failed to enter into BAAs with companies that it retained to provide Internet-based email and calendar services.

In the event of a data breach involving PHI, the HITECH Breach Notification Rule requires a covered entity to notify the Office for Civil Rights (OCR) of the Department of Health and Human Services, affected individuals and in some cases the press. Some breach reports (e.g., those involving 500 or more individuals) typically trigger OCR investigations. State laws also impose breach notice obligations in some cases.

A practice needs to coordinate and in some cases integrate its cloud applications with its IT systems and related policies and procedures. In particular, the practice should update its risk analysis to address security and privacy issues relating to the cloud-based application. The practice should also ensure that it obtains all required patient consents and acknowledgments to appropriate disclaimers, keeping in mind that in December 2014, the FTC announced a settlement with medical billing company PaymentsMD for deceptive trade practices relating to its patient portal for failure to explain the data collected and how the data is used. If a patient portal is used by multiple providers, additional coordination would be needed.

Physician practices need to take care to implement appropriate privacy and security safeguards and perform their due diligence in connection with any cloud vendor relationships.