PLDW
HEALTH CARE

CLIENT ADVISORY:

HIPAA PRIVACY & SECURITY: PRIMER FOR PHYSICIANS

Physicians At Increasing Risk

The HHS Office of Civil Rights ("OCR") has placed physician practices squarely in their sights as they enforce the HIPAA Privacy and Security Rules.

For example, a five-physician Arizona cardiac practice was fined $100,000 for scheduling patient visits on an internet-based calendar. A small Massachusetts dermatology group was fined $150,000 after a thumb drive containing patient records was stolen from a vehicle. This trend can be expected to continue, as the OCR Director has recently responded to OIG criticism by promising to "leverage more civil penalties."

As a quick reminder, HIPAA violations can result in penalties of up to $1.5 million per year, and require notification to the local media. To assist in its enforcement efforts, OCR has established a complaint mechanism for HIPAA violations that Rhode Island patients do indeed utilize. Beyond this, Rhode Island patients have begun to engage legal counsel to find private rights of action in both the common law and the Rhode Island privacy laws.

Understanding A Complex Law

Among other things, HIPAA's Privacy Rule sets forth: the types of information that must be protected; the rights of patients to control access, use and disclosure, as well as to receive certain notices and accountings; and the circumstances under which access, use or disclosure can be made without patient authorization.

HIPAA's Security Rule, by contrast, sets forth the administrative, physical and technical safeguards required to protect patient information. The Security Rule governs electronically stored data, and thus is much more technical in nature than is the Privacy Rule.

Privacy & Security Programs

Both the Privacy Rule and the Security Rule contain requirements regarding organization, documentation and the creation of relevant policies. In fact, the $150,000 fine levied on the Massachusetts dermatology group was partly because they did not have a breach notification policy, and thus failed HIPAA's timeline and notice requirements.

To minimize the risks of a HIPAA violation, and to minimize the potential fine should such a violation occur, a physician practice should have a reasonably-developed HIPAA Privacy & Security Program. While OCR might expect more out of a large, hospital-affiliated group than out of a small practice, there are certain subjects that must be addressed regardless of the practice's size.

Required Program Elements

Security Officer and Privacy Officer

HIPAA mandates that a covered entity have a designated Privacy Officer and Security Officer, although OCR has indicated that one individual can hold both posts.

However, since the Security Officer must have an understanding of the administrative, physical and technical components of the Security Rule, the person assigned to this role must be familiar with the practice's information technology platform.

Policies and Procedures

A practice should have a set of policies and procedures setting forth the obligations of all employees, agents and business associates in safeguarding the privacy and security of patient information. At a minimum, each practice should have a Notice of Privacy Practices, authorizations for release of information, and a breach notification policy that guides both the determination of whether a breach occurred and the decision as to the proper notice procedure.

Underlying these procedural documents should be policies that spell out the manner in which the practice ensures compliance, the steps taken to investigate and, if required, report a suspected breach, and the disciplinary measures attendant upon non-compliance. It is essential that the practice's policies put all employees, agents and business associates on notice that non-compliance may result in discipline up to and including termination.

Risk Assessments and Protections

All covered entities must perform Privacy and Security risk assessments. Given the limited resources of most physician practices, these assessments are routinely performed by outside parties. However, the practice's Privacy & Security Officer(s) must be involved, understand the findings, and participate in the plan to resolve any outstanding issues.

Regardless of practice size, data must at all times remain behind a HIPAA-compliant firewall, be encrypted, or – ideally – both. Just to clarify: the password protection that came with the practice's new laptops or their operating systems almost certainly does not qualify. Similarly, patient-identifying data should never be placed on an unencrypted thumb-drive or disk.

Access to patient information should always require a password, and there should be strong disciplinary measures for the improper sharing of passwords. Employees' access should always be limited to the "minimum necessary" for any individual position, and for each particular access. Employees' access should be immediately terminated when their employment ends or their job duties no longer require access.

External Attacks and Internal Breaches

External hackers consider health information to be the holy grail of personal data, with health information going for as much as ten times more than other personal data on the identity-theft market. Today, the news is filled with stories of million-record thefts from large, institutional entities. However, as these entities devote increasingly-substantial resources to data security, softer targets such as physician groups can expect to become the hackers' next targets.

Further, no firewall or encryption software will protect a practice if a staff member puts patient information into an unencrypted email or text. Every information security system is vulnerable to "points of human interaction," and there is no more dangerous point of human interaction than an unencrypted email or text, be it among staff, to another physician, or even in some cases to the very patient himself.

On the low-tech end of the spectrum, misdirected facsimiles represent a perennial source of HIPAA violations by physician practices. Strategies to auto-load fax numbers and minimize manual dialing can pay large dividends in this area.

Business Associates

Business associates represent a particular vulnerability to physician practices. HIPAA defines a "business associate" as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A business associate is the covered entity's "agent," meaning that the covered entity is liable for what the business associate does or doesn't do on the covered entity's behalf. A physician practice must ensure that vendors who process patient information on its behalf do not put the practice at risk by improperly securing that data.

The first step in ensuring the business associate's commitment to data security is through the use of a Business Associate Agreement ("BAA").

PLDW
HEALTH CARE

HIPAA prescribes numerous assurances that must be contained in each BAA, and failure to secure a proper BAA from each business associate exposes the entity to significant risk.

For example, a hospital in southeastern Massachusetts paid a $750,000 fine after a vendor it hired to dispose of tapes containing patient records lost those tapes. While there was no indication that any patient information was compromised, the fine was levied in part because the hospital did not have a business associate agreement with the transportation company that picked up the tapes on behalf of the similarly-named data-destruction company with which the hospital did have a business associate agreement. Confused? So was the hospital. The lesson here is that the requirements related to BAAs and questions of when they apply are complex and fraught with peril.

Training, Auditing, Discipline & Reporting

The Privacy & Security Officer(s) must ensure that all employees, agents and business associates are adequately educated on the practice's obligations, and each of their individual roles. The structure of the HIPAA Privacy and Security Program should mirror the structure of the practice's Corporate Compliance Program: in addition to the policies and procedures discussed above, there must be top-level commitment, open lines of communication, an ongoing program of training, audit and monitoring, remediation, discipline and, when applicable, reporting of violations.

Benefits Of A Robust Program

The HIPAA Privacy and Security Rules confront physician practices with significant obligations and monetary risks. While "points of human contact" will always leave practices with some level of vulnerability, a robust and well-implemented Privacy and Security Program will go a long way toward both avoiding Privacy breaches and mitigating the consequences should such a breach ever befall the practice.

JOEL K. GOLOSKIE
Of Counsel

Joel K. Goloskie is Of Counsel with Pannone Lopes Devereaux & West LLC and a member of the Health Care, Litigation, and Corporate & Business Teams. His experience ranges from compliance and HIPAA privacy matters to regulatory filings and approvals, contract drafting and management, and mergers and acquisitions. He has assisted health care clients as they dealt with compliance orders and deferred prosecution agreements, and has represented clients in both civil and criminal matters in federal court.

PLDW
PANNONE LOPES DEVEREAUX & WEST LLC
counselors at law

317 Iron Horse Way, Suite 301 Providence, RI 02908
tel 401 824 5100 • fax 401 824 5123