Addressing California's New Privacy Laws: One Organization's Strategy to Handle Stringent Breach Notification Laws

by **Cassi L. Birnbaum** , RHIA, CPHQ

Several well-publicized medical record breaches in California, including the unauthorized access of the governor's wife's record, led to sweeping changes in the oversight, reporting, and enforcement of penalties for privacy breaches in the state. Two new laws signed by Governor Schwarzenegger in fall 2008, and effective January 1, 2009, hold providers, health plans, and individuals accountable for unauthorized access, use, or disclosure of medical information.

The new laws define unauthorized access as the "inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act." Enforcement agencies can fine facilities and individuals up to $250,000 for a data breach. The laws also require that healthcare organizations report privacy breaches to the patient and the California Department of Public Health within five calendar days after discovery of a breach.

With a short window to work within, Rady Children's Hospital of San Diego developed a sound strategy to deal with the requirements of these new laws. The facility's existing privacy policies were consistent with the new laws, and efforts focused largely on reinforcing the message with staff.

Shoring up Privacy Resources

The two bills shot through the state house and assembly and onto the governor's desk in warp speed, giving California hospitals little time to prepare an implementation strategy and review, expand, and reinforce existing policies and practices. Because this wasn't a national initiative, Rady Children's Hospital of San Diego relied on state associations for guidance and collaboration in implementing strategy: the California Hospital Association, California Health Information Association, and the California Privacy and Security Advisory Board.

In addition, Rady shared its approach for implementation as well as its current practices for ensuring compliance with the San Diego Regional Privacy Council. Founded prior to HIPAA implementation, the council's goal is to define, develop, and refine community best practices around privacy and security. Along with sharing educational materials, policies, procedures, and physical and technical safeguards, the San Diego Regional Privacy Council worked on a sanctions and corrective action guideline involving HR departments .

Reinforcing the Foundation with Communication

Review of the new laws against current organizational policies assured Rady that its existing privacy policies were consistent with the new laws. Rady's policy states "unauthorized access, use, disclosure and viewing of medical information is unlawful and subject to sanctions and disciplinary actions up to and including termination."

Three years ago, Rady implemented a proactive monitoring and auditing approach to patient privacy and security to ensure that high-profile and potentially questionable access approaches were flagged and scrutinized. Through this approach, Rady could confirm there was a business need for individuals who accessed records. It has detected breaches in the organization and enabled focused education and performance intervention, including suspension and termination.

A letter signed by the CEO and CMO was sent to the entire work force and physicians about the need to reduce the risk of fines to the organization and to individuals. Rady also reminded the work force of its robust monitoring and surveillance tools to

facilitate the detection of unauthorized electronic record access. A consistent message ran through all messages to Rady's work force that "work force members with access to restricted information are personally responsible for ensuring the confidentiality, privacy and security for data entrusted to them."

Rady also created a Web-based training module targeting the new laws and highlighting compliance best practices and policies. The course is an addition to the annual privacy and security refresher course, which is part of Rady's annual mandatory education curriculum. In addition to making this available to work force members prior to January 1, there were also educational briefings at medical staff, leadership, and department meetings and other forums to help work force members understand the new laws and the consequences of unauthorized access to protected health information (PHI).

The log-in message for the electronic medical record and other systems containing electronic PHI was also updated to include a privacy warning to remind users of their confidentiality obligation.

Rady identified gaps in its existing policies and implemented new strategies to address them. All contracts, agreements, business associate agreements, limited data use agreements, confidentiality agreements, and other arrangements where PHI or electronic PHI is exchanged were revised. This was done to decrease the reporting time when breaches must be reported, define the breach consistent with state law, and ensure the indemnification language is strong enough to cover the maximum fine.

The organization re-evaluated its encryption approach to all devices and reminded its work force that flash drives must be encrypted if they contain PHI and other sensitive information. Rady is also considering a tool that would overlay all electronic PHI systems to streamline its monitoring approach. It is planning a safe disposal event to ensure that outdated or unencrypted CDs, videos, and flash drives are safely destroyed and replaced with compliant devices.

Staff who travel across the county providing care were reminded to make sure that PHI is always in a secure location and in a secure bag to minimize the chance of car break-ins and theft. Although Rady has implemented an electronic record to minimize the amount of paper these staff transport, a few programs performed in conjunction with county or state initiatives still require paper. Some intake forms Rady receives from other agencies contain Social Security numbers. Staff who receive these forms have been instructed to redact this information.

All forms, contracts, and agreements that contain references to PHI or electronic PHI were revised to make sure the language meets the more rigorous standards of the new laws. Rady has also reduced the required breach notification to two calendar days.

Additionally, the organization has met with its key research coordinators and investigators to ensure that they are aware of the new standards and to review the requirements for external transmission of data. Clinical trial agreements and limited data use agreements were updated to reflect the changes in law.

Highlights of California's New Medical Privacy Laws

SB 541 authorizes the California Department of Public Health (CDPH) to investigate health information privacy breaches and assess penalties of up to $25,000 per patient (up to a maximum of $250,000 per reportable event). Health facilities must notify both CDPH and the patient of a privacy breach within five days of detection.

The law also mandates the confidentiality of medical information and requires the implementation of appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information and safeguard it from unauthorized access and viewing, use, or disclosure of medical information. The new law is layered on top of current HIPAA and existing state law.

Reporting Obligations

Facilities covered by the new law must report any unlawful or unauthorized access, viewing, or use or disclosure of a patient's medical information to CDPH and to the patient no later than five days after the unlawful or unauthorized access, use, or disclosure has been detected by the facility.

Penalties for Late Reporting

If a hospital fails to report a detected breach to CDPH or to the patient, CDPH may assess a penalty of $100 per day after the initial five-day period. It is not clear how this late fee will be calculated for late reporting of a breach of multiple patients' records.

Limits on Penalties

The total combined penalty assessed by CDPH for breaches and for late reporting is $250,000 per reported event. "Reported event" covers all breaches included in any single report made by a facility to CDPH, regardless of the number of breach events contained in the report. When CDPH has completed its investigation of a privacy breach, it may refer violations to the Office of Health Information Integrity (OHII).

Investigating Individuals

AB 211, a companion measure to SB 541, authorizes OHII to enforce state medical privacy laws and to assess penalties against individuals for breaches of the Confidentiality of Medical Information Act. However, OHII is not authorized to investigate or fine those facilities subject to SB 541—only CDPH is authorized to investigate and fine those facilities.

OHII will investigate individuals (including physicians, nurses, and medical records clerks) upon receipt of a referral from CDPH. OHII may assess fines against such persons and may also recommend that the person's licensing board (Medical Board of California or the Board of Registered Nursing), if any, investigate or discipline an individual. The licensing board must review any evidence it receives from OHII, but it has discretion regarding whether or not to discipline its licensee.

No News Is Good News

Since the start of the law on January 1, 2009, Rady has not experienced a single breach as defined by unauthorized access, use, and disclosure of PHI. The staff were congratulated for keeping patient information private and secure.

As director of health information and privacy officer I have visited almost every department in a town hall format to allow staff to ask questions regarding the laws and Rady's policies. In return, these sessions provide an in-depth view of their workflow practices and potential risks from a privacy and security standpoint.

At the California Hospital Association annual meeting it was discussed that, based on member feedback, clean-up language would be presented to the California legislature for consideration by May. California covered entities are hopeful this will address some of the gray areas identified and discussed during implementation (e.g., reporting process, guidance on inadvertent disclosure, reporting threshold, fine application).

In the meantime, Rady has tried to reassure anxious staff that they have nothing to worry about if they are taking the necessary precautions with protected and sensitive information and if they are fulfilling a business purpose when handling this information.

State covered entities, represented by the California Hospital Association and the California Health Information Association, are hopeful that California law will be harmonized with the recently passed American Recovery and Reinvement Act to achieve one federal privacy standard, as the key highlights of the legislation include:

- New requirements related to covered entitites and business associates
- A strong new federal security breach notification law
- New guidance for satisfying the minimum necessary standard
- Tighter rules on when protected health information can be used for marketing purposes
- New rules for fund-raising communications
- New measures for accounting for protected health inforamtion disclosures in electronic health records

- Stiffer penalties for noncompliance and heightened federal enforcement

Ultimately, it is important that the pendulum not swing too far in one direction, as this has had a chilling effect on our health information exchange efforts. Constituencies at all levels of the state are working to determine if some type of safe-harbor protection can be obtained for this type of exchange. Meanwhile, the new laws have sounded a wake-up call for the California healthcare work force and its business associates.

Cassi L. Birnbaum (cbirnbaum@rchsd.org) is the director of health information and privacy officer at Rady Children's Hospital of San Diego.

Article citation:
Birnbaum, Cassi L. "Addressing California's New Privacy Laws: One Organization's Strategy to Handle Stringent Breach Notification Laws" *Journal of AHIMA* 80, no.4 (April 2009): 50-51;57.