DECEMBER 2008

CALIFORNIA EXPANDS MEDICAL PRIVACY LAWS WITH NEW STANDARDS, OVERSIGHT, AND ADMINISTRATIVE PENALTIES

On September 30, 2008, California Governor Arnold Schwarzenegger signed two pieces of patient privacy legislation that set forth additional responsibilities for health facilities, clinics, home health agencies, and hospices (collectively, "health facilities") as well as health care providers. Effective January 1, 2009, Senate Bill 541 ("SB 541") and Assembly Bill 211 ("AB 211") require health facilities and health care providers, respectively, to establish patient privacy safeguards and reasonably safeguard patients' medical information against unlawful and unauthorized access. The laws establish new oversight mechanisms and penalties to enforce the patient privacy standards. Health facilities are additionally required to report violations to the state and the affected individual within five days of detection, subject to administrative penalties.

SB 541 and AB 211 were passed in the wake of high-profile privacy breaches at California hospitals. An analysis of SB 541 by the Senate Health Committee cited a 2008 finding by the California Department of Public Health ("CDPH") that UCLA Medical Center employees had accessed hundreds of patients' medical records without authorization, including the records of celebrities such as Farrah Fawcett, Tom Cruise, and Britney Spears. The CDPH also reported that hospitals commonly use patients' information for fundraising purposes without their express permission. The bills are intended in part to clarify that unauthorized access such as "snooping" or other internal misuse of patient records violates state law.

This *Commentary* summarizes how SB 541 and AB 211 affect medical privacy standards and enforcement in California. Affected health facilities and health care providers should review their security and privacy policies in order to ensure compliance with the new state laws.

NEW CALIFORNIA MEDICAL PRIVACY STANDARDS APPLY TO HEALTH FACILITIES AND HEALTH CARE PROVIDERS

AB 211 adds Section 130203 to the Health and Safety Code, which requires health care providers to (1) "establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information" and (2) "reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure." The law covers health care providers as defined in California's Confidentiality of Medical Information Act (the "CMIA"), which includes health care professionals licensed in California and businesses organized for the purposes of making patients' medical information available to patients or providers, such as health care service plans.[1] "Unauthorized access," a new term in California law, is defined as the inappropriate review or viewing of patient medical information without a direct need for diagnosis or treatment or other lawful use. The term effectively covers internal misuses of patients' medical information, such as "snooping" in records by employees and the use of patients' personal data for institutional fundraising without their consent.

SB 541, a companion bill, applies the AB 211 standards to licensed health facilities. The bill adds Section 1280.15 to the Health and Safety Code, which directs that "[a licensed] clinic, health facility, home health agency, or hospice…shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information…consistent with Section 130203." Section 130203, as above, requires covered persons or entities to establish appropriate safeguards to protect medical information and sets forth a reasonableness standard for safeguarding such information from unlawful or unauthorized access.

The expansion of California's medical privacy standards under AB 211 and SB 541 effectively makes much of the federal privacy standard under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") enforceable by state authorities. HIPAA requires covered entities to establish safeguards that limit the internal use of patient data to the minimum extent necessary for employees to carry out the duties of their jobs and reasonably safeguard patient data from unlawful uses.[2] Though substantively similar to the HIPAA standard, the new California laws apply to providers that HIPAA does not. Along with health plans and health care clearinghouses, HIPAA applies to individual or institutional health care providers who transmit health information in electronic form in connection with certain transactions.[3] AB 211 applies to health care providers under the CMIA's definition, which does not require any transmission of electronic health information. Providers not subject to HIPAA may therefore have HIPAA-like obligations under the new California laws.

The expanded California privacy standards will be enforced by new state penalties. AB 211 creates the Office of Health Information Integrity ("OHII"), an enforcement body within the California Health and Human Services Agency that has the authority to investigate potential violations of the AB 211 privacy standards by health care providers. Upon finding an actual violation by a health care provider (*i.e.*, failure to establish appropriate safeguards or reasonably safeguard medical information against unlawful or unauthorized access, as above), OHII may assess penalties as provided in the CMIA, ranging from $1,000 to $250,000.[4] OHII may also recommend the provider to the state's licensing agency for further disciplinary action. SB 541 gives the CDPH the authority to investigate potential violations by health facilities and, when an actual violation of the applicable privacy standard is found, authorizes an administrative penalty of up to $25,000 for each patient whose medical information was accessed unlawfully or without authorization and up to $17,500 for each subsequent occurrence of unlawful or unauthorized access of that patient's medical information, subject to a total cap of $250,000.

---

1 See Civil Code §§ 56.05 and 56.06.
2 45 C.F.R. § 164.514(d), 45 C.F.R. § 164.530(c).
3 45 CFR § 160.102.
4 See Civil Code § 56.36.

The full extent of the data privacy burdens under the new California laws may develop under additional regulations, and California's enforcement strategy will become clearer after the laws take effect on January 1, 2009. Concerned health facilities or providers should consult with legal counsel for specific compliance strategies.

NEW OBLIGATIONS TO REPORT VIOLATIONS OF PATIENT PRIVACY APPLY TO HEALTH FACILITIES

SB 541 requires health facilities to report any violations of the state's data use and disclosure protections to the California Department of Public Health and to the affected patient or patient's representative no later than five days after detecting the incident, subject to a $100 fine for each subsequent day that the disclosure is delinquent. The total fine per reported event for the violation and any reporting delinquency is subject to the above $250,000 cap.

SUMMARY

AB 211 and SB 541 apply new medical information privacy obligations to California health care providers and health facilities, requiring protections from external access and internal misuse. Health facilities must report violations to the state and affected individual within five days of the incident. The new requirements will be enforced by a newly created enforcement body with the authority to issue stiff penalties. In order to comply, affected providers and health facilities should review their security policies and employee education programs, establish the capacity to quickly identify data security breaches, and, if applicable, be prepared to promptly notify the state and affected patients.

AB 211:

- Requires that providers and health plans establish and implement safeguards to protect medical information.
- Requires that providers and health plans reasonably safeguard medical information against access that is unlawful or unauthorized.
- Establishes the Office of Health Information Integrity within the California Health and Human Services Agency and tasks it with investigating violations of the safeguard standards, assessing penalties up to $250,000 per violation, and recommending matters to the state licensing agency for further action.

SB 541:

- Applies the AB 211 safeguard standards to health facilities, clinics, home health agencies, and hospices.
- Requires health facilities, clinics, home health agencies, and hospices to report violations to the California Department of Public Health and the affected individual within five days.
- Sets forth administrative penalties for violating the safeguard standards and the reporting requirement up to a total of $250,000 per reported event.

The full text of AB 211 may be found online at: http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf

The full text of SB 541 may be found online at: http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0501-0550/sb_541_bill_20080930_chaptered.pdf

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

Colin S. Leary
1.415.875.5795
cleary@jonesday.com