



## Psychologists and the Laws Against Snooping

David Leatherberry

Whether working in a private practice, outpatient clinic or an acute psychiatric hospital, mental health providers should be aware that they could be subject to substantial penalties for failing to prevent the unauthorized access of patient medical information. Under two new companion bills that went into effect on January 1, 2009, merely failing to prevent the unauthorized access of confidential patient information, regardless of whether that information is subsequently used or disclosed, may subject the health care provider who is responsible for protecting that information to liability.

Following a year of highly energized media attention to the emotional meltdown of Britney Spears and her brush with involuntary civil commitment and conservatorship proceedings, California legislators have moved to close the gap in privacy laws with respect to so called "snooping." According to the legislative findings published in support of two new companion bills, breaches in medical confidentiality by staff at health care facilities have become increasingly common. Statistics provided by the California Department of Public Health ("DPH") based on investigations done in response to media reports, and cited by the authors of the two bills, demonstrate that more than 120 workers at the University of California, Los Angeles Medical Center viewed celebrity medical records and other personal information without permission between January, 2004 and June, 2008. One individual breached medical record confidentiality 939 times.

According to one media report published in the *Los Angeles Times* (Ornstein, 2008) hospital staff at the UCLA Medical Center often "peeked" into the medical records of prominent patients including celebrities and political figures, and at times engaged in spying into the medical records of other hospital employees. In one such incident that resulted in a DPH investigation, a nurse accessed the psychiatric records of Mariah Carey, and asked the pop singer for an autograph which she later showed to teenaged patients in the hospital. Other episodes of "peeking" reported by the *Los Angeles Times* included access by employees into the medical records of Britney Spears, Tom Cruise, Maria Shriver, Farah Fawcett and the former Beatle star, George Harrison.

In addition to these findings, the DPH found 349 privacy breaches affecting 5,235 patients, and also concluded that despite the 1996 enactment of the federal Health Insurance Portability And Accountability Act (HIPAA), hospitals and other health care organizations were frequently using patient medical information for fundraising efforts without their patients' permission.

### FREE CE CREDIT

CPA Members: Read this article, the Ethics Corner and the four feature articles to earn 2 CE credits. Go to the *Members Only* section of CPA's website ([www.cpapsych.org](http://www.cpapsych.org)) and follow the directions.

Existing California law governing the privacy of medical information is controlled primarily by HIPAA, and the state's Confidentiality of Medical Information Act (CMIA). Under these two legislative frameworks, a covered health care provider is prohibited, with certain exceptions, from using or disclosing protected health information without consent. However, prior to the recent enactment of the two new companion bills, Senate Bill (SB) 541 and Assembly Bill (AB) 211, the penalty for allowing access to such information by someone having no legitimate medical purpose was left unclear.

SB 541, authored by State Senator Elaine Alquist, requires health facilities, including acute care hospitals, psychiatric hospitals, skilled nursing facilities, clinics, hospices and home health agencies to prevent unauthorized or unlawful access, in addition to the unlawful use, or disclosure of a patient's medical information. "Unauthorized" means any inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment or other use permitted by law. While not specifically stated in the bill, such other uses "permitted by law," would include access of patient information for billing and reimbursement purposes, as well as any other exception set forth in the CMIA and HIPAA.

SB 541 provides that the DPH may assess an administrative penalty of up to \$25,000 per patient, and up to \$17,500 for each subsequent access, use or disclosure of that information. As a result, a single unauthorized "viewing" of a patient's medical information by an employee or any other individual – regardless of whether that person intends any harm – may subject the licensed entity to a penalty of \$25,000, in addition to \$17,500 for each disclosure that results from that viewing. The law does not require that each disclosure be from the offending person. Thus, if an employee views a record without authorization and tells two friends, and those friends tell two friends, each disclosure is a separate occurrence. Assuming each disclosure comes to light, the licensed facility could be potentially liable for \$130,000 stemming from a single "peek."

The bill also requires licensed entities to report any unlawful or unauthorized access, use or disclosure of a patient's medical information within five days of discovery to both the DPH and the affected patient or the patient's representative. Failure to report may result in the DPH assessing a penalty of \$100 daily until the report is made, up to a combined maximum penalty of \$250,000. While the \$100 daily penalty may not itself seem significant, failure to report may have a substantial financial impact in that the DPH has substantial discretion based on evidence of a provider's cooperation, good faith efforts to comply with the law, and history of compliance in assessing any penalty. If a provider fails to report the discovery that a record has been accessed without authorization, the DPH may use that failure as a push factor to increase the overall penalty in addition to the penalty of \$100 per day.

While SB 541 itself does not apply to psychologists in private practice, AB 211 creates a separate agency that will have the ability to impose similar administrative penalties against any health care provider, including psychologists, not covered by SB 541. Authored by Assemblymember Dave Jones, AB 211 creates the Office of Health Information Integrity (OHII) to enforce the CMIA, and impose administrative fines against all providers of health care not covered by SB 541 regardless of whether the provider is licensed. As with its companion bill, AB 211 requires a provider of health care to safeguard patient medical information from unauthorized or unlawful access, use or disclosure, using appropriate administrative, technical and physical barriers. The bill effectively clarifies the CMIA to include unauthorized access, and provides a streamlined mechanism for enforcement that did not occur under the legislative framework originally provided by the CMIA. Under AB 211, the OHII will investigate referrals from the DPH, and assess administrative fines as provided by the CMIA. Such fines may range from \$1,000 to \$250,000 in extreme cases. In assessing fines, the OHII will consider whether the defendant provider made a reasonable, good faith attempt to comply with the law; the nature and seriousness of the misconduct; the harm to the patient; the number of violations; the persistence of the misconduct; the length of time over which the misconduct occurred; the willfulness of the misconduct; and the defendant's assets, liabilities and net worth. While AB 211 does not require self-reporting, as is required by SB 541, the persistence factor in determining the penalty suggests that while a psychologist in a private practice need not report the discovery of unauthorized access to the OHII, the psychologist needs to take immediate steps to remedy it.


CalOHII intends to have an official state reporting form for the reporting of privacy violations under AB 211. The form is only in its draft phase. In the meantime, reports may be made by phone to Alan Zamansky at CalOHII, (916) 651-6907. While individually practicing psychologists falling under AB 211 are not required to report discovered privacy violations, CalOHII encourages self-reporting,

and will use the fact that a violation was self-reported as a mitigating circumstance to reduce any penalty that may be assessed. Administrative regulations describing the implementation of AB 211 have not yet been drafted, and will not be available for at least six to nine months.

The intent of the new legislation is to increase the burden on those responsible for protecting patient information so that they will employ appropriate safeguards including administrative, technological and physical barriers that guarantee an individual's right

to privacy. Therefore, psychologists providing patient care in any setting should review their own policies and procedures with respect to the use and disclosure of patient information, and the accessing of such information by staff and other individuals. While this article is not intended to address the mechanics of compliance, or be a substitute for competent legal advice in how best to comply with the requirement of appropriate safeguards, psychologists should consider whether their policies and procedures limit access

to those persons - and at only those times - where access is for a legitimate medical or other lawful purpose. Thus, a policy allowing a receptionist, or temporary agency employee to have access to patient records at their discretion may subject a health care provider to liability under either SB 541 or AB 211. Appropriate policies and procedures should address physical barriers, such as the use of secure storage areas and locking cabinets, as well as technological barriers such as identify verification, auditing of user activity, and lock-out mechanisms to prevent the unauthorized viewing of electronic information. Policies should clarify that accessing patient information without a legitimate medical or other lawful purpose is a violation of employee policies and may constitute a violation of law.

While the imposition of fines against the health care provider may occur based solely on the showing of unauthorized access without regard to whether the access was malicious, the amount of any penalty may be reduced based on a variety of factors including whether the defendant made a good faith attempt to comply with the law. As a matter of prudent practice, therefore, it is important to have appropriate policies and procedures in place. 

## References

Ornstein, C. (2008, April 11). Snooping in records has a history at UCLA, *Los Angeles Times*.

*David Leatherberry is a health care defense attorney in the San Diego office of Gordon & Rees LLP. Mr. Leatherberry is counsel for the San Diego Psychological Association and an adjunct professor in the School of Forensic Psychology at Alliant International University. Mr. Leatherberry was recently recognized with an "Outstanding Attorney Community Service Award" from the Legal Aid Society for his volunteer representation of underserved individuals. Mr. Leatherberry may be contacted by email at [dleatherberry@gordonrees.com](mailto:dleatherberry@gordonrees.com), or contacted by phone at (619) 696-6700.*

---

**Policies should clarify that accessing patient information without a legitimate medical or other lawful purpose is a violation of employee policies and may constitute a violation of law.**

---