

HIPAA Meets Celebrity

By:

Cherilyn G. Murer, JD, CRA

When Congress created the Health Insurance Portability and Accountability Act (“HIPAA”) in 1996, the intention was to create, for the first time, a comprehensive, uniform, patient protection process. The legislation was given teeth – up to \$100 for each violation (which can total hundreds of violations for one investigation), and up to \$25,000 per person in a calendar year. Many feared the HIPAA would lead to relentless Office of Civil Rights investigations, billions of dollars in enforcement costs, and impossible standards for the health care industry to live up to. Reality has been much different, as HIPAA has subtly entered the consciousness of the American health system, it has passed mostly unnoticed into the lives of the Average John or Jane.

For those who are engaged in the health care field, HIPAA has been a pervasive and substantive challenge. Yet, the general public has had very little exposure to HIPAA, beyond the occasional HIPAA privacy notice that is signed during a doctor or dentist office visit. That all changed when singer Britney Spears had her first son, Preston in September 2005.

UCLA Medical Center first disciplined employees, including several employee terminations, when several staff members were “caught prying into records after Spears gave birth...in September 2005 at Santa Monica-UCLA Medical Center and Orthopaedic Hospital.” (C. Ornestein, “UCLA workers snooped in Spears’ medical records,” L.A. Times, March 15, 2008).

The L.A. Times went on to discuss Spears’ recent hospitalization January 31, 2008, and despite earlier memoranda sent to employees to discourage such violations, fired at least 13 employees and suspended at least six others after it was discovered these individuals had accessed Ms. Spears’ non-psychiatric medical records. Interestingly, UCLA disclosed that Ms. Spears’ psychiatric records had not been accessed, due to heightened record security for the UCLA neuro-psychiatric hospital.

It should not be believed that this crackdown was the first – indeed employees have been subjected to internal disciplinary action since HIPAA’s Privacy Rule became effective in 2003. Before Britney, there was the situation of the 27 employees of Palisades Medical Center in North Bergen, New Jersey, who were suspended for accessing George Clooney’s medical records after his motorcycle accident. Before Clooney, there was Tri-City Medical Center in Oceanside, California that left 10 employees without a job after accessing, photographing, printing and sharing an X-ray within the hospital without consent.

In all, Britney Spears was not the first high-profile HIPAA violation, but the tremendous public spotlight on her life has re-focused the healthcare world on important questions: How safe are our electronic and hard-copy medical records? If there is a HIPAA violation, what can be and what is being done about it?

It may surprise some to learn that the pop star has, albeit unintentionally, instigated a broader examination of HIPAA violations. But HIPAA, as a relatively new law, was festering behind the curtain, waiting for a high-profile patient privacy violation before enforcement could truly begin.

So why has there not been any fines yet assessed from a HIPAA violation? Part of the reason is the multiple bureaucratic hurdles facing the Office of Civil Rights and Centers for Medicare and Medicaid Services.

HIPAA Enforcement

Complaints

The process for which OCR complaints are processed was codified in 45 USC §160 et. al. in the February 16, 2006 Federal Register (FR Vol. 71, No. 32). Only a “covered entity” is subject to HIPAA penalties, defined as a health care provider, health care clearinghouse, or health plan. Pursuant to HIPAA regulations, a person who believes a covered entity is not complying with HIPAA requirements may file a complaint with HHS. The filing must be in writing (paper or electronic), name the person responsible and the basis for the complaint, and be completed within 180 days of when the complainant knew or should have known that the act occurred. As with many other sections of the regulations, HHS may waive the time limit for good cause.

The Secretary of HHS is then charged with the authority to investigate these complaints with a review of the pertinent policies, procedures or practices of the covered entity and of the circumstances surrounding the alleged violation. HHS may also conduct compliance reviews, seemingly at their discretion, to determine whether covered entities are complying with the applicable HIPAA regulations. Such compliance review, although without procedural limitations as to when or where HHS will conduct such reviews, would include informal (and formal if necessary) notification to the covered entity. The first HHS compliance review is believed to have taken place in March 2007 at Piedmont Hospital in Atlanta, Georgia (J. Vijayan, “HIPAA audit at hospital riles health care IT”, *ComputerWorld*, June 15, 2007), and others are expected to follow.

The Office of Civil Rights (“OCR”) will often oversee the entire HIPAA Privacy Rule Complaint Process. In rare occasions, after their initial investigation, OCR may refer the complaint to the U.S. Department of Justice. This would generally result if there are identity theft issues or other criminal issues. The Department

of Justice will then either accept the case, or decline and refer the investigation back to OCR.

Noncompliance

The point at which a covered entity should become increasingly concerned is if HHS determines noncompliance with HIPAA following an investigation of a compliant or a compliance review. HHS will notify the covered entity if the noncompliance is not resolved by informal means. The covered entity then has 30 days to submit written evidence of any mitigating factors or affirmative defenses. If after the informal, then formal investigation, HHS is still unsatisfied as to compliance, they will then notify the covered entity of such finding in a written notice. At this point civil money penalties are a potential resolution to the noncompliance, and the covered entity is on the verge of joining an unwelcomed club - becoming the first to receive such a monetary fine.

Civil money penalties (“CMP”) may be assessed against a covered entity if any “agent,” or workforce member of the entity commits the violation. Generally speaking, the agency provision does not extend liability to a covered entity if there exists a business associate agreement between the covered entity and the agent.

While the per-violation amount may seem insignificant, the financial impact will range depending on the violation. For example, one employee of a hospital that violates the Privacy Rule by inappropriately accessing Patient A’s chart, would represent a single violation. However, if a hospital’s electronic medical records system has substantial security flaws, it is conceivable for an employee to access hundreds, even thousands of patients’ data.

Despite the potential for monetary penalties, HHS would be unlikely to fine a small health system the maximum amount if the violation were partially attributable to mitigating factors.

HIPAA compliance – Factors to consider in determining the amount of a civil money penalty:

➤ The nature of the violation, in light of the purpose of the rule violated
➤ The circumstances, including the consequences, of the violation, including but not limited to <ol style="list-style-type: none">1) The time period during which the violation(s) occurred;2) Whether the violation caused physical harm;3) Whether the violation hindered or facilitated an individual’s ability to obtain health care; and4) Whether the violation resulted in financial harm.
➤ The degree of culpability of the covered entity, including but not limited to: <ol style="list-style-type: none">1) Whether the violation was intentional; and2) Whether the violation was beyond the direct control of the covered

entity.
<ul style="list-style-type: none"> ➤ Any history of prior compliance with the administrative simplification provisions, including violations by the covered entity, including but not limited to: <ol style="list-style-type: none"> 1) Whether the current violation is the same or similar to prior violation(s); 2) Whether and to what extent the covered entity has attempted to correct previous violations; 3) How the covered entity has responded to technical assistance from HHS provided in the context of a compliance effort; and 4) How the covered entity has responded to prior complaints
<ul style="list-style-type: none"> ➤ The financial condition of the covered entity, including but not limited to: <ol style="list-style-type: none"> 1) Whether the covered entity had financial difficulties that affected its ability to comply; 2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and 3) The size of the covered entity.
<ul style="list-style-type: none"> ➤ Such other matters as justice may require

Source: 45 CFR § 160.408

In addition to the many considerations above, HHS may not impose a fine if the covered entity has an affirmative defense: no knowledge of the violation (even had the entity exercised reasonable diligence), or the violation is due to reasonable cause and not willful neglect and is corrected within 30 days of knowledge.

After all of the potential remedies, if HHS still imposes a fine and notifies the covered entity as such, the covered entity may still request a hearing before an administrative law judge on the proposed penalty. If this ALJ hearing is requested, publication of such a fine will not occur until the proposed penalty is finalized by the ALJ.

With such an extensive process which must precede government imposition of a civil monetary fine, it is no wonder that no fine has yet been passed down and finalized by HHS.

Complaint Increases

Although the above describes the framework for how HIPAA complaints and violations are handled by the federal government, it is far more common for these issues to be addressed internally by a health system. Therefore while no fines have yet been assessed by HHS, there are extensive anecdotal stories of such issues being addressed internally with warnings, suspensions, and even firings.

While the majority of HIPAA concerns appear to be addressed within health systems through their grievance procedure, there are increasing indications that patients, who fear a breach of their health data confidentiality, are not satisfied by internal investigations and corrective actions and still report the complaint to the government. This could lead to more active OCR investigations into HIPAA complaints as the volume of reported violations continues to rise.

Even without the imposition of the first HHS fine for a HIPAA violation, OCR letters are becoming more common, and more substantive. When asked about the over 30,000 HIPAA complaints and zero fines, HHS Secretary Michael Leavitt responded that the point of HIPAA is not to fine doctors or hospitals, but to make sure they comply with the law (P. Van Osdol, "HIPAA Secretary Not Happy with Violations," WTAE TV Channel 4, March 12, 2008). However, in the interview Secretary Leavitt noted there could be fines issued in the future.

It is heartening that HIPAA compliance regulations are drafted in a manner that encourages compliance and protection of medical records, as opposed to focusing on immediate and aggressive penalties. Government should be in the business of guiding health care towards better outcomes and safety, not geared towards civil and criminal action for those who make a mistake that oftentimes is unintentional.

Nevertheless, HIPAA does provide the tools for enforcement that should be taken seriously. It is only a matter of time before the Office of Civil Rights makes an example of a health care provider, pursuing all available penalties against the covered entity that recklessly disregards HIPAA.

However, the driving force for compliance with HIPAA regulations should not be governmental penalties, but rather the universal desire to protect the privacy of patients and ensure the provision of quality health services.

About the Author:

Cherilyn G. Murer, J.D., C.R.A. is CEO and founder of the Murer Group, a legal based healthcare management consulting firm in Joliet, IL, specializing in strategic analysis and business development. Ms. Murer may be reached at (815) 727-3355 or viewed on her web site: <http://www.murer.com>