PUBLICATION

OCR Settles with Shasta Regional Medical Center for $275,000 [Ober|Kaler]

2013: Issue 13 - Focus on HIPAA/Privacy

The HHS Office of Civil Rights (OCR) recently announced a $275,000 settlement with Shasta Regional Medical Center (SRMC) on the heels of an investigation triggered by a *Los Angeles Times* article indicating that senior hospital officials had disclosed information regarding a patient's treatment without her consent.

In addition to the monetary settlement, SRMC was required to execute a one-year Corrective Action Plan (CAP) that requires SRMC to modify its policies and procedures, retrain its employees, and submit annual reports. The CAP also requires that 16 facilities related to SRMC submit to OCR an attestation indicating that they understand that an individual's PHI remains protected even when it has been disclosed by the individual herself or otherwise made a part of the public record and that disclosures of PHI to the media *always* require the patient's authorization.

SRMC's troubles began in the wake of an investigation of its billing practices. *California Watch*, a California news outlet following the billing investigation, reported that the hospital had billed for treating a patient for a severe form of malnutrition (even though the patient was overweight and indicated she received no such treatment). In response, hospital executives (acting through SRMC's parent company, Prime Healthcare) released the patient's medical record to several media outlets, with at least one executive claiming that the patient "waived" her privacy rights when she discussed her care with the media. The OCR disagreed.

SRMC's Violations

OCR's Resolution Agreement (RA) (which also attaches a copy of the CAP) provides some detail regarding the categories of noncompliance it identified as justifying the monetary settlement and CAP:

- SRMC "failed to safeguard the [patient's] PHI" from impermissible disclosure when it intentionally released the patient's record to *California Watch*, *The Record Searchlight*, and the *Los Angeles Times*;
- SMRC impermissibly used the patient's information when it sent an email to its entire workforce containing much of the same information shared with the media outlets; and
- SRMC "failed to sanction its workforce members pursuant to its internal sanctions policy which requires that it sanction employees for 'violations of HIPAA.'"

SRMC's CAP

A settlement with OCR generally requires not only a cash payment but also a commitment to a (generally, two-year) Corrective Action Plan. These plans are intended to ensure ongoing compliance much in the same fashion as Corporate Integrity Agreements are intended to ensure ongoing compliance following a settlement with the HHS OIG. The two agreements also obligate the provider to significant ongoing reporting and auditing responsibilities, as well as potentially substantial costs related to a diversion of enterprise resources and the retention of (and satisfaction of) an outside auditor.

Notably, the CAP requires that SRMC correct its policies and procedures (with regard to both disclosures and discipline) and submit them for approval, submit annual reports, and retrain its employees; but it does not require the engagement of an outside monitor, the submission of monitor reports, or the imposition of any (announced or unannounced) site inspections. Interestingly, the CAP also requires that the 16 *other* facilities owned and operated by Prime Healthcare submit attestations indicating that they are aware that the HIPAA implementing regulations prohibit the disclosure of a patient's medical record to a media outlet without the patient's authorization, even where the record has been requested by the media.

In the event that SRMC fails to fulfill its responsibilities under the CAP, of course, SRMC would remain subject not only to an additional investigation and any penalties resulting from the conduct that breached the CAP, but OCR would no longer be bound by the settlement's release.

Ober|Kaler's Comments

The SRMC settlement is instructive in several ways:

- It appears difficult to argue with OCR's determination in this case – the facts behind the disclosure, and the reported statements of the hospital's officials are not in dispute. Sending a patient's medical records to a news organization without the patient's authorization does not seem to be a "grey" area of HIPAA compliance, even if the patient has already spoken of the underlying medical condition publically.
- HIPAA compliance is not an issue which can be relegated to "compliance people." Compliance is enterprise wide. Every employee (including senior management) should have a familiarity with HIPAA and its regulations (and facility policies) sufficient to accomplish their work in a compliant manner and to notice when issues implicating privacy concerns arise. Not everyone needs to be a Privacy Officer, but everyone should know when to call the Privacy Officer.
- Policies and procedures, including policies concerning sanctions and discipline, must be followed, even if senior management must be sanctioned. Such sanctions can be undertaken by the organization's Board of Directors as necessary.
- The size of a breach doesn't necessarily dictate OCR's reaction. While every breach of more than 500 patients will be investigated, OCR may, and will, investigate smaller breaches where it believes it has good cause.

* *Joshua J. Freemire is a former member of Ober|Kaler's Health Law Group*