THOMPSON
INFORMATION SERVICES

• COMPLIANCE
• ASSURANCE
• SUCCESS

June 5, 2015

A Practitioner Takes PHI to a New Employer: **Is It a Breach?**

By GERALD "JUD" DELOSS

A Rochester, N.Y., hospital recently issued breach notices to more than 3,000 patients when one of its nurse practitioners took their protected health information to her new employer. Based on the facts described by the hospital, however, it is not clear that a reportable breach actually occurred.

When the nurse informed the University of Rochester Medical Center that she was leaving to take a position with Greater Rochester Neurology, she asked URMC for a patient list "to help ensure continuity of care for the patients she was leaving," according to URMC's notification letter. URMC did not object and provided the patient list to the nurse. She then shared the list with GRN, which "used the list to send letters to patients, informing them that the nurse practitioner was joining their practice and advising them of the option to be treated at their facility."

Was There a HIPAA Violation?

To trigger HIPAA's breach notification requirements, there first must be a use or disclosure of PHI that violates HIPAA's privacy rule (see the *Guide to Medical Privacy & HIPAA*, ¶860). HIPAA allows covered entities to disclose PHI to a health care provider for the provider's treatment activities.

URMC indicated that providing the PHI to the nurse practitioner was acceptable under HIPAA. But arguably, the same analysis would apply when the nurse practitioner in turn shared the information with her new employer, also a health care provider, to ensure continuity of care.

Both the nurse practitioner and the neurology group/new employer are health care providers under HIPAA, and "treatment" includes coordination or management of health care and related services by one or more health care providers (see ¶421). The letters sent to each patient informing them that the nurse practitioner joined the neurology group, and offering the patient the option to continue to be treated by the nurse practitioner at her new employer, would appear to fall within the definition of "treatment."

Low Probability That PHI Was Compromised

Even if the disclosure did violate HIPAA, URMC might well have been able to overcome the presumption of a reportable breach by showing there was a low probability that the PHI was compromised. Recall that to do so, under the 2013 final omnibus rules, a covered entity must conduct a risk assessment that applies this four-part test:

1. the nature and extent of the PHI involved;
2. the person who used the PHI or to whom it was disclosed;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated. (See ¶862, and related breach evaluation tool.)

Here, according to URMC's notice the PHI was not of a sensitive nature. It was disclosed to a neurology group, a health care provider and

Clark Hill attorney **Gerald "Jud" DeLoss**

continued on page 2

continued from page 1

covered entity. The neurology group did actually acquire and presumably viewed the PHI. However, according to URMC, the neurology group returned or destroyed the PHI, it was not shared with anyone else and it was used only to communicate directly with patients regarding continuity of care. This all would appear to weigh against a finding of risk to the PHI.

In the preamble to the 2013 rules, the U.S. Department of Health and Human Services gave the example of a covered entity that sends a fax containing PHI to the wrong health care provider. If the provider notifies the sender and destroys the PHI, there is a low probability that the PHI has been compromised.

If the provider notifies the sender and destroys the PHI, there is a low probability that the PHI has been compromised.

The underlying rationale for HHS' conclusion was that the recipient had an obligation to maintain the PHI's confidentiality and returned/destroyed it, so it would not be used for improper purposes. Likewise, as URMC noted, the recipient in this instance was a health care provider and covered entity that is prohibited from using or disclosing the PHI improperly and, in fact, did return or destroy all of the PHI without any further use or disclosure.

For these reasons, the situation involving URMC may not have risen to the level of an unauthorized disclosure, and URMC arguably had no obligation to provide a HIPAA breach notification — although it may have had state-law or purely reputational reasons for doing so.

Gerald "Jud" E. DeLoss is a member in Clark Hill PLC's Chicago office in the health care practice group. Jud focuses on the representation of behavioral healthcare providers, hospitals, medical groups, federally qualified health centers, trade associations, health information exchanges, EHR vendors and research organizations. His practice areas include health information privacy, HIPAA, corporate transactions, regulatory compliance, reimbursement, contracting and credentialing/privileging. Jud is a member of the Guide to Medical Privacy & HIPAA editorial advisory board. **Contact him via phone: (312) 985-5925 or email: gdeloss@clarkhill.com.**