HEALTH LAW ALERT

July 31, 2009

HIPAA-steria - The Sequel
First Up: Breach Notification

By Katherine B. Kravitz, Esq.

The new federal stimulus bill, “ARRA1,” includes the HITECH Act2, which contains, among other things, an expansion of HIPAA privacy law requirements for health care providers. The HIPAA provisions go into effect on a rolling schedule over the next several years, and further guidance for compliance will be forthcoming over that time period. Since much is still unknown, hospitals and other health care providers may wish to go about tackling the technical maze of new requirements (and avoiding HIPAA-steria) with an equally graduated, and systematic approach to enforcement. This Alert will focus on the breach notification provision, which is scheduled to go live in September of 2009.

General Rule. Under HITECH, any hospital or other covered entity which maintains protected health information (PHI) must notify the patient in the event of a breach of the data. Importantly, this provision only applies to data which is “unsecured;” if a breach of “secured” data occurs, no notification is required.

What is a Breach? A breach is the unauthorized access, use or disclosure of PHI which compromises the security or privacy of the information. There are, however, some important exceptions. For example, a disclosure may not be a breach requiring notification if you would not expect the person to whom the information was disclosed to remember it. This could cover a misdirected fax, depending upon the procedures followed. Also, if an employee acting in good faith, within the scope of his/her job duties, improperly accesses a record, as in the case of inadvertent or accidental access, this is not reportable so long as there is no further disclosure.

What makes data “secure?” Per DHHS’ April 27th guidance, electronic data is “secure” if encrypted as further specified in the HIPAA Security Rule and in guidelines promulgated by the National Institute of Standards of Technology and available at http://www.csrc.nist.gov/. The encryption method should use a process which transforms data into a form “in which there is a low probability of assigning meaning without the use of a confidential key or process.” As for hard copy records, per the guidance that hard copy PHI is only “secure” if destroyed in a manner which makes it unreadable.

Form/Timing of Notification. Notification must be made in writing, by mail or e-mail if that is the patient’s preference. The notification must be made within 60 days of discovery of the breach. If the breach involves disclosure of PHI of 500 or more people, notification also must be made to the media and to DHHS, and the incident will be posted on a DHHS public website.

---

1 American Recovery and Reinvestment Act of 2009
2 Health Information Technology for Economic and Clinical Health Act
Further Guidance to Come/Start Date. On or before August 16, 2009, DHHS is to publish final interim rules on breach notification. In its April guidance, DHHS asked for public comments, and the final interim rules are expected to address industry comments and concerns. These rules will then apply to breaches occurring 30 days after the publication of the rules, or no later than September 15, 2009.

Next Steps. Hospital and other health care providers should consult with their health care professional to flesh out a plan for HITECH compliance. Some things to consider in making your plan include:

• Review of Business Associate agreements to ensure that BA’s are required to give timely notice of breaches to allow for your compliance with HITECH’s 60 day deadline for notification.
• Review of most common breach circumstances and reportability; does every misdirected fax require a breach notification? This must be thoroughly analyzed and a policy created to supplement your existing HIPAA compliance program. Policies should be worded broadly enough to allow for analysis of each individual situation.
• Education. While staff may be aware of the need for privacy of PHI, these new requirements, along with HITECH’s substantially increased financial penalties, put a much greater emphasis on the importance of maintaining confidentiality on a day to day basis.

The Future. At the American Health Lawyers Annual Meeting in early July, a representative from the OCR addressed the agency’s enforcement philosophy, saying, “I love the word reasonable,” when asked about the new HIPAA provisions. The commitment to this philosophy will be borne out in the coming months and years.


Kathy Kravitz, a partner at Barley Snyder, has served as counselor to Barley Snyder’s health care clients for nearly 20 years. Her practice covers the full range of issues affecting health care providers including HIPAA, EMTALA, scope of practice and licensure issues, end of life issues, risk management, mental health procedures and the numerous state and federal regulations governing health care providers. Kathy also has an active litigation practice, and has successfully defended health care providers against malpractice claims in a number of counties across central Pennsylvania. Kathy also represents health care providers before the State Licensing Boards as well. She can be reached at kkravitz@barley.com; 717-399-1533.

Barley Snyder’s Health Law Group represents hospitals, health systems, long-term care facilities, continuing care retirement communities, physicians, and other health care providers with their increasingly complex legal needs. Our health care attorneys have broad experience in trial advocacy as well as current clinical and health care issues. For more information about Barley Snyder’s Health Law Group, please visit www.barley.com.

This communication is provided as a general informational service to clients and friends of Barley Snyder LLC. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered ATTORNEY ADVERTISING in some states. If you have updates to this mailing list, email barley@barley.com with your specific requests.