Melancon, Downey & Hall, LLC

May 31

Mr. Fredric Adair
Chief Compliance Officer
Patton – Fuller Community Hospital

Mr. Adair:

In response to your request for an update of HIPAA privacy and security requirements, here is a brief update.

Data Privacy

As you know, HIPAA requires that covered entities such as a hospital keep all personal health information (PHI) private. Information should only accessed by those who need to provide clinical care, or used by insurers to pay claims, or by business associates as required by contract. Those accessing personal health information (PHI) should only use the minimum necessary information they need to provide care, pay claims, or provide appropriate clinical services.

Data Security

HIPAA security requirements require that the organization review the administrative safeguards, physical safeguards, and technical safeguards which can be put in place to secure data. The organization should consider its size, resources, and staff capabilities in putting a data security plan in place. The organization does need to identify all electronic personal health information (EPHI), have policies and procedures in place, have a security plan in place based on what is reasonable for the organization, and regularly re-assess data security risks.

HITECH Act Secured and Unsecured Data

As you know, the 2009 stimulus bill included the HITECH Act which made changes and updates to HIPAA. Business associates are now directly subject to HIPAA as well as HIPAA enforcement penalties. In addition, HHS has set forth rules about breach notification when there is a breach of data privacy or security. A distinction is made between "secured data" which has been encrypted or destroyed so as to be undecipherable.

If there is a HIPAA breach that involves secured data, then the security of the data protects the information so that no harm results and there are no further requirements. On the other hand, if the data is "unsecured data" then the possibility that PHI may be wrongfully accessed is present. The organization is then required to analyze whether the use and disclosure of PHI violates HIPAA privacy; whether the disclosure results in risk to the financial, reputational, or other harm to the individual; and whether any HIPAA exceptions would apply.

For example, if PHI is inadvertently disclosed, say a patient letter is sent to the wrong address, but there is no indication the recipient had knowledge of the PHI, say the letter was returned unopened; then there would be no harm from the breach and no further action would be required. However, if it appears that the data disclosure or security breach could lead to access of the PHI, then further action is required.

HITECH Act Breach Notice Requirements

When it is determined that there was a breach of unsecured PHI, then the hospital is under obligation to provide notice of the breach. Each individual whose unsecured PHI has been acquired, accessed, used or disclosed as a result of the breach must be notified within 60 calendar days of the discovery of the breach. If for some reason, the contact information is not available for 10 or more individuals, then substitute noticed must be given by posting a notice on the corporate web page for 90 days.

In addition, if the breach impacted more than 500 residents in the state, then notice of the breach must be given to prominent media outlets within 60 calendar dates of the discovery of the breach. Also, when more than 500 residents in the state are involved, the hospital must notify HHS concurrently with individual notifications.

Should the hospital be required to provide breach notification, I would be glad to provide assistance on the specifics required.

Sincerely,

Beverly Downey
Managing Partner