Stanford Health Privacy Breach Highlights Downstream Vendor Risks, Issues

October 7, 2011

In an earlier post I described a HIPAA privacy breach that occurred when a spreadsheet detailing the emergency room treatment of nearly 20,000 patients of Stanford Hospital was posted online, for the better part of a year, at a "homework for hire" website, www.studentoffortune.com. The New York Times has published an article tracing the breach to a job applicant who received the spreadsheet from a one-person marketing agency hired by the Hospital's third party billing contractor.

The spreadsheet was originally transmitted in encrypted format from the Hospital to the marketing agent, who had represented himself as a vice-president of the billing contractor and was in fact the hospital's main contact for the billing contractor. In fact, he was not an executive of the billing contractor, but the billing contractor nonetheless condoned his use of that title in order to get access to various health executives and generate customers for its billing services. The marketing agent unencrypted the spreadsheet and provided it to the job applicant with the request that she demonstrate her skills converting it to bar graphs and charts. Without recognizing that the names and treatment codes on the spreadsheet were "real world" data, the job applicant then sought help with the assignment by posting the spreadsheet on www.studentforhire.com, where it was discovered almost a year later by the parent of a Hospital patient named in the chart.

In other words, the breach was not attributable to a Hospital employee, or an employee of the Hospital's business associate, the billing contractor, but to a "downstream vendor" or "subcontractor" of the billing contractor, and not even to an employee of the downstream vendor but to a mere job applicant. One of the patients disclosed in the spreadsheet has since sued Stanford Hospital and the billing vendor in L.A. County Superior Court, seeking damages of $1,000 for each of the 20,000 affected individuals.

This is a frightening object lesson for covered entities – the Stanford Hospitals of the world – and for business associates such as the billing contractor – about the risks presented by "downstream" vendors, and the need to ensure that their handling and use of protected health information and e-PHI meets HIPAA and applicable state law privacy and data security standards. HIPAA as amended by HITECH now demands that business associates vouch in this manner for their downstream vendors in their business associate agreements. Clearly, to do so, the parties first must clearly identify downstream vendor relationships, and not disguise the vendor's staff as business associate employees, as occurred in the Stanford case. Even where the vendors clearly are identified, business associates should also address, in business associate agreements, whether the covered entity can share data directly with the downstream vendors, and if so, under what conditions. The Stanford case is unusual due to the disguising of the marketing agent's true status, but it suggests that business associates might always want to be at least notified of such communications, if this is administratively practical. Or, they might want to vouch for privacy/security compliance only when data passes through them to the downstream vendor, but require the covered entity to be responsible for breaches resulting from its direct communications with the downstream vendors.

Trying to stay ahead of the technological curve in data transmission is almost impossible, but we can learn from others' mistakes and take whatever steps are necessary not to repeat them.

I:\cpr\Articles\Stanford Health Privacy Breach Highlights Downstream Vendor Risks.doc