KRIEG DEVAULT

Insights

Hybrid Entities: The Importance of Properly Designating Health Care Components

December 11, 2016

By: Stephanie T. Eckerle

The United States Department of Health and Human Services, Office for Civil Rights ("HHS") and the University of Massachusetts Amherst ("UMass") recently entered into a Resolution Agreement and Corrective Action Plan to settle HIPAA violations resulting from the impermissible disclosure of electronic protected health information ("ePHI"). The breach resulted from a workstation in the UMass Center for Language, Speech and Hearing (the "Center") that was infected with a malware virus resulting in the disclosure of ePHI, including names, diagnosis and procedure codes.

Although UMass considers itself a hybrid entity, the underlying problem in the case at bar resulted from UMass allegedly not designating the Center as a covered health care component. Pursuant to HIPAA, a hybrid entity is defined as a covered entity "(2) Whose business activities include both covered and non-covered functions; and (3) That designates health care components in accordance with § 164.105(a)(2)(iii)(D)." [1]

The covered entity must take care to designate and segregate all health care components in the hybrid entity, which can require the implementation of significant infrastructure and monitoring to comply with the hybrid entity requirements. [2]

For example, the covered entity must take care to maintain the appropriate documentation regarding the health care components of the hybrid entity and retain that documentation for six years from the date of its creation or the date when it was last in effect, whichever is later. [3]

In the UMass case, because UMass allegedly failed to designate the Center as a covered health care component, other HIPAA requirements were not undertaken by UMass. This included an alleged failure to have the proper policies and procedures, risk analysis and technical security measures in place. The Corrective Action Plan resulting from these issues requires UMass, among other things, to "conduct a comprehensive and thorough Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by UMass." [4]

The Risk Analysis must then be provided to HHS and UMass must create "an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis described above." [5]

The UMass Resolution Agreement and Corrective Action Plan is a warning to all hybrid entities to ensure that they have properly designated their health care components and are complying with all other HIPAA rules. [6]

A copy of the Resolution Agreement and Corrective Action Plan can be found here.

Please contact Stephanie T. Eckerle to discuss this matter, or if you have any questions.

1. 45 CFR § 164.103

2. 45 CFR § 164.105

3. 45 CFR § 164.105(c)
4. CAP, p. 2
5. CAP, p. 3
6. 45 CFR § 164.105