Subject: Million Dollar Reminder
Date: Thursday, March 17, 2016 8:17:44 AM

Good morning –

This settlement of $1.55M is a good reminder of why we all work so hard to ensure we have a Business Associate Agreement in place with our vendors who access our PHI and why Jonathan Cox is working diligently with each of you on our risk assessment. Please note that OCR made these findings as part of an investigation into another violation involving an unencrypted laptop. Once an investigation is opened, all policies and practices are subject to review. In this case, the covered entity was (among other things) allowing a vendor to access its EMR without having a BAA in place. All vendors who access OU's PHI – for maintenance, audit, report generation, etc. -- must have signed a BAA *prior* to accessing the PHI.

Please share with those in your area who are involved in the vendor selection/contracting process or risk assessment process, as well as your clinic managers and Tier 1s – they are in one of the best positions to assist with these items. Let me know if you have any questions.

Thanks.

Jill

From: Raines, Jill (HSC)
Sent: Thursday, March 17, 2016 7:56 AM
To: Raines, Jill (HSC)
Subject:

North Memorial Health Care of Minnesota has agreed to pay $1,550,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

"Two major cornerstones of the HIPAA Rules were overlooked by this entity," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). "Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure."

OCR initiated its investigation of North Memorial following receipt of a breach report on September 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the electronic protected health information (ePHI) of 9,497 individuals.

OCR's investigation indicated that North Memorial failed to have in place a business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf. North Memorial gave its business associate, Accretive, access to North Memorial's hospital database, which stored the ePHI of 289,904 patients. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that it maintained, accessed, or transmitted across its entire IT infrastructure -- including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

In addition to the $1,550,000 payment, North Memorial is required to develop an organization-wide risk analysis and risk management plan, as required under the Security Rule. North Memorial will also train appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan.

The Resolution Agreement and Corrective Action Plan can be found on the HHS website at: https://urldefense.proofpoint.com/v2/url?u=http-3A__www.hhs.gov_hipaa_for-2Dprofessionals_compliance-2Denforcement_agreements_north-2Dmemorial-2Dhealth-2Dcare_index.html&d=BQIFaQ&c=qRnFByZajCb3ogDwk-HidsbrxD-31vTsTBEIa6TCCEk&r=Uwzi50RQ7KVJAWE2DA3HmxgYBLC3wV3nwXD68IY8jsU&m=UwCcnPf07SXtx2O_6nOmPviD6Xz16UgePRsCtEU02xQ&s=sN7S-JocWEYcPYODcjo2JEX3M-fzQfWEAVaftWe-bs4&e= .

Jill Bush Raines
Assistant General Counsel and
University Privacy Official
University of Oklahoma
(405) 271-2033 / 271-1076 fax