**Subject:** OCR Guidance Related to IT Security and HIPAA Security
**Date:** Tuesday, August 02, 2016 11:08:22 AM

Good morning -

Please review the following recommended actions from the Office for Civil Rights and consider what additional steps your areas put in place to assist your campus with compliance with the recommended actions, particularly those that are highlighted.  Please share with others in your area who may be affected by these recommendations.

Thank you.

Jill

Jill Bush Raines

Assistant General Counsel, Office of Legal Counsel

and University Privacy Official

The University of Oklahoma

1105 N. Stonewall Avenue, Suite 221

Oklahoma City, OK  73117-1221

(405) 271-2033

(405) 271-1076 (fax)

jill-raines@ouhsc.edu

CONFIDENTIALITY NOTICE: This email, which includes any files transmitted with it, contains confidential information from University Legal Counsel, is intended solely for the use of the individual or entity to whom it is addressed, and may contain information protected by the attorney-client privilege.  If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited.  If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of this email and any attached files.

-----Original Message-----
From: OCR HIPAA Privacy Rule information distribution

August 1, 2016

Do You Know Who Your Employees Are?

Insider threat is becoming one of the largest threats to organizations and some cyberattacks may be insider-driven.  Although all insider threats are not malicious or intentional, the effect of these threats can be damaging to a Covered Entity and Business Associate and have a negative impact on the confidentiality, integrity, and availability of its ePHI.  According to a survey recently conducted by Accenture and HfS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption.  Further, it was reported by a Covered Entity that one of their employees had unauthorized access to 5,400 patient's ePHI for almost 4 years.

US CERT defines a malicious insider threat as a current or former employee, contractor, or business partner who meets the following criteria:

* has or had authorized access to an organization's network, system, or data;

* has intentionally exceeded or intentionally used that access in a manner that negatively,

affected the confidentiality, integrity, or availability of the organization's information; or information systems.

According to a survey conducted by U.S. Secret Service, CERT Insider Threat Center, CSO Magazine, and Deloitte, the most common e-crimes committed by insiders are:

* unauthorized access to or use of organization information;

* exposure of private or sensitive data;

* installation of viruses, worms, or other malicious code;

* theft of intellectual property.

Covered Entities and Business Associates should consider:

Ø  Following US CERT steps to protect ePHI from insider threats:

1. Consider threats from insiders and business associates in enterprise-wide risk assessments.

2. Clearly document and consistently enforce policies and controls.

3. Incorporate insider threat awareness into periodic security training for all employees.

4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

5. Anticipate and manage negative issues in the work environment.

6. Know your assets.

7. Implement strict password and account management policies and practices.

8. Enforce separation of duties and least privilege.

9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

10. Institute stringent access controls and monitoring policies on privileged users.

11. Institutionalize system change controls.

12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.

13. Monitor and control remote access from all end points, including mobile devices.

14. Develop a comprehensive employee termination procedure.

15. Implement secure backup and recovery processes.

16. Develop a formalized insider threat program.

17. Establish a baseline of normal network device behavior.

18. Be especially vigilant regarding social media.

19. Close the doors to unauthorized data exfiltration.

Resources: US-CERT https://urldefense.proofpoint.com/v2/url?u=http-3A__resources.sei.cmu.edu_library_asset-2Dview.cfm-3FassetID-3D34017&d=CwIFaQ&c=qRnFByZajCb3ogDwk-HidsbrxD-31vTsTBEIa6TCCEk&r=Uwzi50RQ7KVJAWE2DA3HmxgYBLC3wV3nwXD68IY8jsU&m=OWaWL2a3CV4CUjs6fkbum4fg53o9tAj1V2hO7Celi1c&s=QuMGD5WNwRN3rNivEvgrSzNnoxSNbSw7sfS6fdh3aKc&e=

###

************************************************************************

End of OCR-PRIVACY-LIST Digest - 27 Jul 2016 to 1 Aug 2016 (#2016-31)

********************************************************************