COMMITTED TO
EXCELLENT CLIENT SERVICE

HANCOCK
ESTABROOK, LLP
COUNSELORS AT LAW

OCTOBER 2018
www.hancocklaw.com

HEATH CARE LAW ALERT

HIPAA SECURITY REVIEW OF MOBILE DEVICES

The increasing use of removable media in the health care setting, including laptops, tablets, smart phones and USB drives (collectively "Mobile Devices"), put HIPAA Covered Entities and Business Associates at risk of experiencing a breach if Mobile Devices are not properly secured. In fact, unsecured Mobile Devices have been the focus of several recent HIPAA settlements with the Office of Civil Rights ("OCR"), the federal agency that enforces HIPAA.

While many entities have considered routine risks to electronic PHI on their networks, some have failed to consider evaluation of Mobile Devices specifically. The HIPAA Security Rule (45 CFR §§ 164.302-164.318) does not mandate any particular technological solutions for the protection of ePHI, including ePHI contained on Mobile Devices. Rather, entities are required to maintain "reasonable and appropriate" administrative, technical, and physical safeguards for protecting ePHI. OCR has published a number of guidance documents revealing what it considers to be "reasonable and appropriate" safeguards for Mobil Devices, including the following:

- **Administrative Safeguards**
    - Risk Analysis: Mobile Devices should be included in an enterprise-wide risk analysis with follow-up actions to reduce risks identified with the use of Mobile Devices to a reasonable and appropriate level.
    - Risk management: Entities should review the security of Mobile Devices regularly and modify procedures as necessary to ensure ePHI remains protected. With respect to Mobile Devices that leave the premises, OCR offers the following as "reasonable and appropriate" risk management strategies:
        - Implement policies and procedures regarding the use of Mobile Devices, including policies on: mobile device management; using your s
        - own device; restrictions on mobile device use; and security or configuration settings for Mobile Devices;
        - Consider using Mobile Device Management (MDM) software to manage and secure Mobile Devices;
        - Identify the types of hardware and electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or

digital memory cards, and security equipment and develop inventory control systems;
        - Implement processes for maintaining a record of the movements of, and person(s) responsible for, or permitted to use hardware and electronic media containing ePHI;
        - Require authentication to use or unlock Mobile Devices;
        - Install or enable encryption, anti-virus/anti-malware software, and remote wiping capabilities;
        - Regularly install security patches and updates;
        - Consider the use of biometrics, such as fingerprint readers, on portable devices;
        - Securely delete all PHI stored on a mobile device before discarding or reusing devices; and
        - Include training on how to securely use Mobile Devices.
    - Sanction Policy: A sanction policy must be in place and effectively communicated so that workforce members understand the consequences of failing to comply with the security policies and procedures related to offsite use of, or access to ePHI.

- **Physical Safeguards**
    - Workstation Use/Security: Unrestricted access to USB ports and removable media devices can facilitate unauthorized copying of data to removable media, as well as permit access to removable media which could be infected with malicious software. OCR suggests that effective controls to protect ePHI might include port and device locks that physically restrict access to USB ports or CD/DVD drives and technical controls, including Microsoft Windows Group Policy configuration and third party software.

- **Technical Safeguards**
    - Encryption and Decryption: Although encryption is an "addressable" specification, OCR guidance states that Mobile Devices should be encrypted.
    - Audit Controls: The HIPAA Security Rule does not identify what information should be collected from an audit log or trail or how often the audit reports should be reviewed, but entities must consider their risk analysis results and organizational factors, such as their current technical infrastructure, hardware, and software security capabilities.

The risks of downloading PHI onto unencrypted Mobile Devices are clear. There have been multiple settlements between OCR and organizations involving unencrypted thumb drives. For example, OCR recently reached a settlement for $4.3 million dollars with MD Anderson Cancer Center related to 3 separate breaches involving the theft of an unencrypted laptop and two unencrypted USB thumb drives. The breaches impacted over 33,500 individuals.

In a settlement totaling $1.55 million dollars, OCR considered not only the loss of an unencrypted, password-protected laptop including PHI of 9,497 individuals, but also the Covered Entity's failure to conduct a complete risk analysis to address the risks to PHI

maintained across its entire IT infrastructure, including all mobile devices and electronic media.

In another example, a breach involving stolen USB devices containing PHI of 2,209 individuals ultimately led to OCR imposing a penalty of $2.2 million. The penalty appears to have increased because OCR's investigation revealed that the entity had failed to conduct a risk analysis and implement a risk management plan, contrary to the entity's representations.

Covered Entities and Business Associates would be wise to take steps toward improving security for ePHI stored on Mobile Devices through an organization-wide risk analysis of such devices. Password protection alone is insufficient; thus, additional steps might include using encryption technology for drives where PHI might be copied onto Mobile Devices. It is equally important to ensure that policies and procedures are in place regarding the use of Mobile Devices. If such policies already exist, they must be followed consistently.

Covered Entities and Business Associates must include Mobile Devices in their organization-wide risk analysis, and build off the risk analysis to adopt safeguards that will secure PHI stored on these devices. OCR is unlikely to be tolerant of entities that have failed to take these basic steps to secure Mobile Devices when reviewing a breach.

References:

- OCR January 2017 Cybersecurity Newsletter, *Understanding the Importance of Audit Controls*, available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html
- OCR October 2017 Cybersecurity Newsletter, *Mobile Devices and Protected Health Information (PHI)*, available at: https://www.hhs.gov/sites/default/files/october-2017-ocr-cybersecurity-newsletter.pdf
- OCR Fact Sheet, *Managing Mobile Devices*, available at: https://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf
- December 28, 2006 DHHS Security Guidance document available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf?language=es.

If you have any questions or would like more information on the issues discussed in this communication, please contact any of the following Hancock Estabrook attorneys:

Raymond R. D'Agostino	315.565.4518	rdagostino@hancocklaw.com
Catherine A. Diviney	315.565.4520	cdiviney@hancocklaw.com
Marguerite A. Massett	315.565.4537	mmassett@hancocklaw.com
Mary M. Miner	315.565.4542	mminer@hancocklaw.com
Carrie J. Pollak	607.391.2860	cpollak@hancocklaw.com
Briana K. Wright	315.565.4562	bwright@hancocklaw.com