Is ePHI Encryption Required? The Failure to Properly Protect ePHI Can be Quite Costly

(June 27, 2018): Violations of the Health Insurance Portability and Accountability Act (HIPAA), where a Covered Entity[3] has failed to utilize ePHI encryption can be quite costly. The loss of unencrypted electronic media containing Protected Health Information (PHI)[1] can result in big fines as one Texas medical center has recently learned the hard way. As a case ruling issued earlier this month reflects, the University of Texas MD Anderson Cancer Center (MD Anderson) was fined $4.3 million for their loss of two unencrypted USB drives and theft of an unencrypted laptop. This article examines this case in more detail and discusses your obligations to protect electronic PHI (ePHI) from improper disclosure or access by unauthorized persons.

I. Is ePHI Encryption Required by Covered Entities?

The Department of Health and Human Services (HHS) oversees compliance and enforces HIPAA's sanctions for noncompliance through its Office for Civil Rights (OCR). In cases involving possible criminal conduct, the OCR works with the Department of Justice (DOJ).

The HIPAA Omnibus Rule has changed the enforcement provisions.[2] Previously, the agency had discretion in choosing whether to investigate complaints or potential violation in cases where the Agency's preliminary review reveals a *possible* violation due to willful neglect. Now, the agency is required to initiate a formal investigation when a party appears to have exhibited willful neglect. If an investigation is performed, it may include a review of pertinent policies, procedures, or practices of the Covered Entity and the circumstances of the alleged violation. Documentation and evidence of compliance are key to ensuring no penalties are assessed by OCR.

Notably, the HIPAA Omnibus Rule modified HIPAA's Privacy, Security and Enforcement Rules in order to implement the statutory amendments set out under the Health Information Technology for Economic and Clinical Health Act (HITECH). Under HITECH, a Covered Entity is required to conduct a comprehensive ***"security risk analysis"*** of the administrative, physical, technical and operational aspects of your organization. For each category, the Security Rule establishes both required and addressable implementation specifications.

Implementation specifications that are identified as required must be fulfilled by a Covered Entity. The failure to implement ***required*** specifications will be automatically deemed to be a failure to fully comply with the requirements of the HIPAA Security Rule. In contrast, specifications that are identified as ***addressable*** must only be implemented if, after a risk assessment, the Covered Entity has concluded that compliance with the specification is a reasonable and appropriate security risk safeguard for handling PHI and ePHI.

Contrary to popular belief, Covered Entities are not mandated by law to encrypt ePHI. As the security risk assessment implementation specification covering encryption is expressly noted as an addressable specification, it is not required. As ***45 C.F.R. §164.312(a)(2)(iv)[4]*** expressly provides:

> ***"(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information."***

Clear as mud? If you are still confused as to your obligations, you aren't alone. Although you may determine that it would be reasonable for you to ***NOT*** encrypt a certain set of ePHI, you need to keep in mind that if there is a potential breach (through loss, theft, negligence, etc.) the OCR will be second-guessing your decision-making in this regard.

II. The Encryption "Safe Harbor":

Section 13402 of HITECH extended the privacy provisions of HIPAA by requiring that Covered Entities and their business associates notify affected individuals after discovering breaches of unsecured PHI.[5] Breach, in this case, means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the information.[6] Generally, incidents within the Covered Entity (between employees) or unintentional disclosure to a business associate are not breaches. Thus, if an employee sends an email inappropriately but in good faith containing PHI to a co-worker and neither employee shares it with others, it is not a breach. If the email goes to someone who is not an employee of the entity or a business associate, it may well be.

Furthermore, the breach notification requirements apply only to "unsecured PHI**"**— meaning PHI that is not secured through the use of technology or methodology specified by the Secretary, such as encryption or destruction that renders the paper unusable, unreadable, or indecipherable.[7] Therefore, if a Covered Entity encrypts information to comply with the Security Rule and subsequently discovers a breach of that information (through loss, theft, accidental delivery to the wrong person, etc.), the Covered Entity is ***not*** required to provide notice of the breach. If the information is protected through a firewall or some other means not approved by the Secretary, then notification would be required for a breach. To ensure encryption keys are not breached, they should be kept on a separate device from the data to which they apply.

III. The MD Anderson Case:

In the MD Anderson case, the cancer center supposedly lost two unencrypted flash drives and experienced the theft of an unencrypted laptop. Collectively, the devices were estimated to have contained the PHI of approximately 33,500 patients. The OCR alleged that the cancer center did not comply with regulatory requirements by:

> ***"(1) failing to perform its self-imposed duty to encrypt electronic devices and data storage equipment; and (2) it allowed ePHI to be disclosed. "***

Pursuant to 45 C.F.R. pt. 160 and 45 C.F.R. pt. 164, subpts. A, C, D, and E, Covered Entities are generally required to:

> ***"ensure the confidentiality, integrity, and availability of all ePHI that the entities create, receive, maintain, or transmit; protect such information against any reasonably anticipated threats or hazards to its security; protect ePHI against any reasonably anticipated impermissible uses and disclosures; and ensure compliance with these requirements by their workforces."***

While the cancer center had policies and procedures for maintaining the safety of ePHI, it was alleged that they did not implement those as required by 45 C.F.R. § 164.312(a)(1). MD Anderson argued that they satisfied this regulation because there were technically policies and procedures put in place to allow PHI to be encrypted. MD Anderson's procedures for protecting ePHI included:

1. ***Password protection of all computers and portable computing devices accessing potentially confidential information;***
2. ***A requirement that confidential or protected data stored on portable computing devices must be encrypted and backed up to a network server in the event of a disaster or loss of information;***
3. ***Annual employee training event that provided its employees with training in areas that included ePHI transmission and proper disposal; a prohibition against password sharing; a discussion of password necessity and integrity; an explanation of authorized and proper use of information systems, and training about information security resources.***

Unfortunately, MD Anderson's policies and procedures in this regard were shown to be incompletely or ineffectively implemented. The laptop and two USB drives in question were not encrypted as required by the cancer center's policies and procedures. MD Anderson's attempts

to ensure implementation of its ePHI protection policies and procedures were characterized as "*half-hearted*" by the ALJ handling the case. MD Anderson was found to have delayed the encryption of devices and, after years, only proceeded slowly with the implementation of the encryption policy claiming financial issues were to blame.

The laptop in question was being used by a telecommuting employee as work computer and it was neither encrypted nor password protected. The laptop was stolen from the home of the employee and the ePHI was vulnerable although no breeches in the security of the patients concerned in the PHI resulted. The first USB concerned was lost by a trainee while on an employee shuttle bus. The second USB was lost by a visiting researcher.

The OCR considered the theft of the laptop and the losses of the USB flash drives to be unlawful disclosures of ePHI because these actions constituted the "*release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information*."

IV. Defenses Raised by MD Anderson:

In its defense, the cancer center raised a number of arguments before the ALJ, several of which are outlined below.

- **As a State Entity, MD Anderson is Not a "Person" as Defined Under HIPAA.** In addition to arguing that the Secretary, HHS had acted beyond the authority of the position, MD Anderson also argued that as an entity of the State of Texas, it did not constitute a "person" and was therefore not covered under HIPAA. The ALJ disagreed.

- **The Penalties Assessed by the Secretary Were Excessive.** Secondly, MD Anderson argued that any penalties assessed should be capped at $100,000 per year. The cancer center also cited 45 C.F.R. § 160.546(b) and asked that the ALJ reduce the assessed penalties to below the statutory cap. Notably, the ALJ refused to lower the penalties imposed by the Secretary, HHS, claiming that doing so would *"constitute an end run around the Secretary's intent as expressed in the regulation."* **[8]** The ALJ also cited 45 CFR 160.408 which allows aggravating factors such as the general pursuit of justice to dictate fine amounts. Additionally, MD Anderson also claimed that the high penalties imposed were a violation of the excessive fines provision outlined in the 8th Amendment. Not surprisingly, the ALJ responded that it did not have the authority to consider the constitutionality of the ruling. Each of MD Anderson's arguments were addressed in the ALJ's decision.

- **The Theft and Loss of Devices Do Not Constitute a "Disclosure" Under HIPAA.** MD Anderson further argued that stolen or lost property cannot constitute a "*disclosure*" of sensitive material mainly because there is no evidence the PHI was viewed by anyone. However, the mere fact that the PHI was compromised and rendered vulnerable to viewing

by an unauthorized person was deemed enough to constitute a disclosure in violation of HIPAA. Finally, the cancer center argued that the behavior of the individuals who lost USB drives was unsanctioned along with the actions of the thief. Therefore, there was no basis to hold MD Anderson responsible for these unauthorized acts. Not surprisingly, the ALJ disagreed, holding that although the employees may have disobeyed MD Anderson's policies, the actions of transporting the data were within the scope of their official duties.

- **The OCR Has Failed to Apply HIPAA's Regulations Consistently.** Among concern by the Texas Cancer Center that their key arguments were not seriously considered, there was also concern that the OCR's enforcement of HIPAA regulations is not transparent or consistent[9]. With the Texas Cancer Center's fine being the 4th largest ever upheld, there seems to be merit to the claim that regulations are not being consistently or fairly enforced. For example, in a 2010 case involving Rite Aid, the large national drug store chain agreed to pay $1 million to settle HIPAA privacy violations after several of its pharmacies were videotaped disposing of prescription pill bottle labels which contained identifying information into dumpsters with public access[10]. It seems odd when comparing the two cases that one of the nation's largest drug store chains was fined less than one quarter of the amount of fines assessed against MD Anderson for the violations discussed above.

V. Next Steps for MD Anderson:

MD Anderson Cancer Center has expressed plans to appeal the ALJ's ruling[11]. The cancer center feels not only that the $4.3 million in fines is too much but that the ruling does not take into account the policy and procedure the center had already created. At the end of the day, however, it isn't the availability of a mechanism to keep ePHI safe that matters but that strong efforts are made to ensure ePHI is actually being protected. Failing to carry out policy and procedure can bring serious fines.

VI. Steps You Can Take to Comply with Your Obligations Under HIPAA and HITECH:

- **Compliance Officer.** Appoint a Compliance Officer for your organization.
- **Breach Insurance.** Review your options for purchasing insurance to cover any damages and penalties that may result from an unintentional breach or unauthorized disclosure.
- **Notice of Privacy Practices.** Ensure that an updated *Notice of Privacy Practices* is in place.
- **Patient Consent Form.** Ensure that an appropriate "*Patient Consent Form*" is in place.
- **Business Associate Agreements.** Ensure that an appropriate "Business Associate Agreement" is in place with each of the outside entities with whom you use or disclose PHI. Additionally, check with your business associates and verify that they understand their obligations and will only provide any subcontractors access to your ePHI with your permission. Will you require that your business associate obtain breach insurance?

- **Policies and Procedures.** Review and update all of your policies and procedures required to meet your obligations under HIPAA and HITECH to comply with the law and implement safeguards to protect the integrity of the individually identifiable health information under your control:
    - Privacy Rule;
    - Security Rule;
    - Enforcement Rule;
    - As mandated in connection with your Security Risk Analysis;
    - Other policies and procedures needed to address risks involving social media, using your own cell phones, telecommuting, etc.
- **ePHI Encryption.** Review your operational practices to ensure that ePHI is encrypted to prevent improper use or disclosure. Although encryption may not be mandated, it is essential if you are trying to reduce your organization's level of risk.
- **Backup Procedures.** Review your backup procedures and ensure that in the event of a disaster or other unforeseen event, a complete encrypted copy of your patient's ePHI is safely maintained.
- **Security Risk Analysis.** Perform / update the Security Risk Analysis of your organization and assess any outstanding specifications that still need to be met. Additionally, review the risks and vulnerabilities of a potential breach and / or the wrongful disclosure of ePHI.
- **Employee Training.** Ensure that all of your staff is trained on their obligations to comply with HIPAA's requirements under the law. Furthermore, ensure that all new members of your staff are trained on their obligations under the law within 30 days of entering on duty.
- **Minimum Necessary.** Review your use and disclosure practices to ensure that the minimum necessary standard is being met.
- **Breach Response Plan**. Develop a breach response plan (including, but not limited to breach notification when needed, analysis of the cause of the breach, remedial steps and any additional staff training that may be needed), to better ensure that your organization can effectively respond to a breach incident.

Robert W. Liles **serves as Managing Partner at Liles Parker, Attorneys & Counselors at Law. Is your organization dealing with a potential HIPAA breach or unauthorized disclosure? For a free initial consultation, contact Robert or one of the other attorneys at Liles Parker. 1 (800) 475-1906.**

[1] The term *"Protected Health Information"* (PHI) covers individually identifiable health information that is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. The rules do not include "de-identified information," individually identifiable information where all 18 identifiers have been removed. Such information can be used without restriction or patient authorization. The following table describes the identifiers that must be removed in order to qualify as de-identified information.

18 Individual Identifiers

1 Names	**10 Account numbers**
2 All geographic subdivisions smaller than a state, except for the initial three digits of a ZIP code if the geographic unit formed by combining all ZIP Codes with the same 3 digits contains more than 20,000 people.	