On January 18, 2017, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced a HIPAA settlement with the MAPFRE Life Insurance Company of Puerto Rico related to impermissible disclosure of electronic protected health information (ePHI). The settlement requires MAPFRE to pay a $2.2M resolution amount and institute a corrective action plan. The settlement highlights the importance of a robust security management process, particularly as it relates to administrative, physical, and technical safeguards for portable electronic devices (PED) that store ePHI.

The facts underlying the settlement are common to many recent enforcement actions. In September 2011, MAPFRE reported to OCR that a USB data storage device containing 2,209 individuals’ ePHI (including complete names, dates of birth, and Social Security numbers) had been stolen from the company’s IT department, where it had been left overnight. According to the breach report, the company had been able to identify the breached ePHI by reconstituting it on the computer to which the PED had been attached.

OCR’s investigation into MAPFRE’s compliance with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) indicated the following conduct occurred:

- Impermissible disclosure of 2,209 beneficiaries’ ePHI, in violation of the HIPAA Privacy Rule;[1]
- Failure to conduct a Security Rule risk analysis (an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI) and implement a risk management plan (security measures sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level);[2]
- Failure to implement a security awareness and training program for all workforce members;[3]
- Failure to implement a mechanism to encrypt ePHI;[4]
- Failure to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other HIPAA Rule requirements to safeguard ePHI.[5]
The corrective action plan requires MAPFRE to conduct a Security Rule risk analysis incorporating “all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by MAPFRE Life and its Workforce … that contain, store, transmit, or receive MAPFRE Life ePHI.” As part of this process, MAPFRE must develop a complete inventory of all electronic equipment, including PEDs, data systems, and applications that contain or store ePHI. OCR must then approve MAPFRE’s risk analysis. MAPFRE must also develop and implement a Security Rule risk management plan (RMP) to address and mitigate any security risks and vulnerabilities identified in the risk analysis. The RMP must include a process and timeline for implementation, evaluation, and revision. OCR must also approve the RMP, as well. MAPFRE must revisit the risk analysis annually, and document the security measures it implements to reduce the identified risks and vulnerabilities to ePHI to a reasonable and appropriate level.

In addition to conducting an initial and annual risk analysis and implementing a risk management plan, MAPFRE must develop a process to evaluate environmental or operational changes affecting the security of ePHI. Upon OCR’s approval of this process, MAPFRE must implement it, including distributing it to workforce members with responsibility for performing the evaluations.

The corrective action plan requires MAPFRE to review and, as necessary, revise its Privacy Rule and Security Rule policies and procedures to ensure they comply with the HIPAA Rules. MAPFRE must distribute the policies and procedures to all workforce members with access to ePHI, as well as to current and future HIPAA business associates (BA). MAPFRE must assess and, as necessary, update and revise its policies and procedures at least annually. The policies and procedures must, at a minimum, address:

- Uses and disclosures of ePHI as described in the Privacy Rule;
- Privacy Rule and Security Rule training for workforce members;
- The Security Rule security management process (risk analysis, risk management plan, workforce sanction policy, and information system activity review);
- Security Rule device and media controls;
- Security Rule policies and procedures;
- Encryption and decryption; and
- Workstation use.

Finally, MAPFRE must implement an OCR-approved workforce training program, providing training at least annually and within 30 days of a workforce member beginning service.

MAPFRE will be subject to a 3-year compliance oversight program by OCR.

Commenting on the settlement, OCR Director Jocelyn Samuels noted: “Covered entities must not only make assessments to safeguard ePHI, they must act on those assessments as well. OCR works tirelessly and collaboratively with covered entities to set clear expectations and consequences.”

What Should Covered Entities and Business Associates Do Now?

The $2.2M resolution amount is one of OCR’s highest – and it was negotiated to balance potential violations against evidence of MAPFRE’s financial standing. Given the small size and relatively common nature of the breach, the resolution amount and 3-year monitoring period send a strong message to regulated entities: OCR
has a low tolerance for breaches of unencrypted ePHI, particularly when the breach results from the loss or theft of a PED. Several of OCR’s most recent-high dollar settlement involved precisely such breaches: St. Joseph Health, Advocate Health Care Network, University of Mississippi Medical Center, and Oregon Health & Science University occurred in 2016 alone and involved multi-million dollar settlements with each regulated entity. Advocate Health paid $5.5M to resolve alleged breaches resulting from, among other things, the theft of unencrypted laptops from the premises and a workforce member’s vehicle. The takeaway? Using PEDs to store and transmit ePHI can greatly benefit health care and is in many respects an industry standard, but regulated entities must never become complacent.

Covered entities and business associates have had all the time OCR is going to give them to put administrative, physical, and technical safeguards in place to protect ePHI stored and transmitted on PEDs. If a breach results from unencrypted ePHI on a lost, stolen, or compromised portable electronic device, the covered entity or business associate may find itself subject to stringent enforcement. While there is no substitute for full and complete compliance with the Privacy Rule, Security Rule, and Breach Notification Rule, there are several foundational steps CEs and BAs can and should take now to protect themselves and the patients and beneficiaries they serve.

1. **Build your compliance program “by design,” with basic Security Rule tenets informing each step.** The Security Rule charges covered entities and business associates with (a) safeguarding the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; (b) protecting against reasonably anticipated threats or hazards to security or integrity; (c) protecting against reasonably anticipated uses or disclosures that would violate the Privacy Rule; and (d) ensuring workforce compliance.[6] While the Security Rule is technology-neutral and allows regulated entities to take a flexible approach to compliance,[7] CEs and BAs should ensure their leadership and workforce are familiar with these basic duties, as well as the underlying concepts of confidentiality, integrity, and availability:

   a. **Confidentiality** means data is not made available or disclosed to unauthorized persons or processes.[8]

   b. **Integrity** means data has not been altered or destroyed in an unauthorized manner.[9]

   c. **Availability** means data is accessible and usable upon demand by an authorized person.[10]

   Building these concepts and basic tenets into each aspect of your security and privacy compliance program – from concept, to design, to implementation and beyond – will help ensure a firm foundation upon which to build specific privacy and security measures.

2. **Create an organization-wide data map.**

   It is difficult, if not impossible, to safeguard the confidentiality, integrity, and availability of ePHI when you do not know it exists. Mapping the location of ePHI, and how it flows into, within, and out of the organization, is a necessary first step of a robust compliance program. This can be accomplished in a variety of ways depending on the size and scope of your organization, your workforce structure and responsibilities for ePHI, and the technology you use. A good lesson from the MAPFRE settlement, however, is that your data map must include an inventory of all
3. **Implement a robust security management process for ePHI.**

A foundational element of a regulated entity’s Security Rule compliance program is an administrative safeguard known as the security management process (SMP). The SMP consists of policies and procedures to prevent, detect, contain, and correct security violations, and is implemented through:

a. **Risk analysis.** Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, integrity, and availability of ePHI held by the covered entity (CE) or BA;

b. **Risk management.** Implementing security measures sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level;

c. **Sanction policy.** Applying appropriate sanctions against workforce members who fail to comply with security policies and procedures; and

d. **Information system activity review.** Implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The goal of the SMP is to identify risks and manage them to a reasonable and appropriate level (not to “zero” – an impossible task).

4. **Emphasize your risk analysis.**

The foundation upon which the SMP rests is the risk analysis. It is impossible to overstate the importance of an accurate, thorough, enterprise-wide investigation into risks and vulnerabilities that may affect ePHI. While the Security Rule requires a risk analysis, it does not tell CEs and BAs how to perform it. OCR recently issued guidance to assist regulated entities with this task. While OCR is clear that the guidance does not provide a “one-size-fits-all blueprint for compliance,” it does clarify OCR’s expectations for organizations working to meet the requirements. A robust risk analysis can inform critical decisions within the organization, such as appropriate personnel screening processes; when and how to back up data; whether and how to use encryption; when data must be authenticated to protect integrity; and the appropriate manner of protecting ePHI transmissions – to name a few.

The core of the risk analysis is identifying vulnerabilities and risks to ePHI. A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited by a threat, resulting in a security breach or violation of the entity’s security policy. [13] Vulnerabilities may be technical (e.g., holes, flaws, or weaknesses in the development of information systems, or incorrectly implemented or configured information systems), or non-technical (such as ineffective or non-existent policies, procedures, standards, or guidelines). A threat is the potential for a person or thing to accidentally trigger or intentionally exploit a specific vulnerability.[14] Threats may be natural (floods, earthquakes, tornadoes), human (network or computer based attacks, malware upload, unauthorized access to ePHI), or environmental (power failures, liquid leakage). A risk is the net mission impact, considering the likelihood that a threat will accidentally trigger or intentionally exploit a vulnerability (probability), and the degree of resulting effect.
The data map is critical to determining the scope of the risk analysis. An RA must encompass all ePHI that the organization creates, receives, maintains, or transmits, regardless of its form of electronic medium, source, or location. The regulated entity can create the data map using such techniques as reviewing past and existing projects, interviewing workforce members and BAs/subcontractors, reviewing documentation, and using other data gathering techniques. The CE or BA must document the data mapping process.

After identifying risks and vulnerabilities, the organization must assess whether required security measures are in place, and whether they are configured and used properly. OCR emphasizes that security measures implemented to reduce risk will vary among organizations – for example, the security measures a small organization implements may look very different from those in a larger organization due to differences in workforce size and degree of internal control.

Appropriate security measures will also vary according to the entity’s assessment of probability and criticality. CEs and BAs must safeguard against “reasonably anticipated” risks to confidentiality, integrity, and availability. This involves not only identifying threats, but accounting for probability – or how likely it is that a threat will exploit a vulnerability, resulting in risk. Entities must also account for criticality – the degree of impact that will result if the threat actually exploits the vulnerability. The organization may use qualitative or quantitative measures of potential impact. Measuring probability and criticality will allow the CE or BA to assign risk levels for threat and vulnerability combinations, and formulate a risk management plan to mitigate each risk level.

As for the RMP itself, note that the Security Rule is technology-neutral. In deciding what security measures to use to safeguard the confidentiality, integrity, and availability of ePHI, CEs and BAs may consider their size, complexity, and capabilities; their technical infrastructure, hardware, and software security capabilities; the cost of the anticipated security measures; and the probability and criticality of potential risks to ePHI (i.e., how likely is a threat to manifest, and how serious an impact to confidentiality, integrity, and availability would result)?

The CE or BA must document the results of its risk analysis and resulting RMP. No specific format is required.

Finally, the risk management process is not “one and done.” Rather, OCR expects the regulated entity to conduct continuous risk analysis and identify when updates are needed. The frequency of this process will vary among organizations, but a “truly integrated” risk management process is performed “as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation.” In other words, CEs and BAs should incorporate “risk management by design” into their administrative, physical, and technical environments. OCR’s guidance states:

For example, if the covered entity has experienced a security incident, has had a change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and adjusting risk management processes to address risks in a
timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

5. **Carefully consider encryption.**

The Security Rule requires “transmission security” for ePHI: the CE or BA must “implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”[24] The Security Rule transmission security standard involves both integrity controls[25] and encryption – or their functional equivalent.

Encryption is a method for converting plain text to encoded text by means of an algorithm. If data are encrypted, there is a low probability that anyone other than the receiving party – who has the key necessary to translate the encoded text – would be able to decrypt. CEs and BAs are often surprised to find that encryption is an “addressable” implementation specification for transmission security, and mistakenly believe they can freely choose to not implement encryption. This belief is simply false, and espousing it can be a sure path to entity and patient harm, and significant OCR enforcement.

When an implementation specification is “addressable,” the CE or BA must:

- Assess whether the specification is reasonable and appropriate in the entity’s environment, considering its “likely contribution” to protecting ePHI; and
- Implement the specification, if reasonable and appropriate, and if not, document why and implement “an equivalent alternative measure” if reasonable and appropriate.[26]

Therefore, you must encrypt ePHI “whenever deemed appropriate,” [27] unless you can demonstrate that encryption is not a reasonable and appropriate security measure within your specific organizational environment. If encryption is not reasonable and appropriate for your organization, you must implement an “equivalent alternative” transmission security measure to guard against unauthorized access to the unencrypted ePHI being transmitted over an electronic communications network (or, if no reasonable and appropriate equivalent alternatives exist, otherwise meet the transmission security standard). You must carefully document the results of your analysis.

While the Security Rule does not therefore *actually* require encryption, it does *effectively* require this technical safeguard for ePHI – because there are few, if any, organizational environments in which encryption would not be reasonable and appropriate. First, consider the risk to patients and the organization if ePHI is not encrypted. Second, consider the result if OCR audits you and disagrees with your assessment that encryption is not reasonable and appropriate. Third, consider that encryption is an effective “safe harbor” under the Breach Notification Rule, because ePHI encrypted to NIST standards is not “unsecured PHI” – and the BNR requires reporting only for breaches of unsecured PHI. Each of these considerations strongly favors encryption.

6. **Implement device and media controls.**

The MAPFRE settlement is not the first to result from a lost or stolen PED. The Security Rule requires CEs and BAs to implement policies and procedures governing the receipt and removal of hardware and electronic media containing ePHI in and out of the facility, and their movement within the facility. [28] To implement the device and media controls physical security standard, covered
entities and business associates should address:

- **Disposal.** Implement policies and procedures to address disposal of ePHI and the hardware and electronic media on which it is stored;
- **Media re-use.** Implement procedures for removing ePHI from electronic media before making the media available for reuse;
- **Accountability.** Maintain a record of the movements of hardware and electronic media, and any person responsible for them; and
- **Data backup and storage.** Create a retrievable, exact copy of ePHI, when needed, before moving equipment.[29]

Encryption may prevent a breach if a portable electronic device is lost or stolen. Certain device and media controls work in concert with encryption to prevent breaches in the event of loss or theft (e.g., the disposal and media re-use controls), and others may prevent loss or theft in the first place. For example, an entity’s “accountability” policies and procedures may forbid removal of ePHI-containing PEDs from the premises, or may forbid workforce members from leaving these devices unattended in their vehicle.

7. **Train your workforce.**

Both the Privacy Rule and the Security Rule require workforce training. The Security Rule requires CEs and BAs to “[i]mplement a security awareness and training program for all members of its workforce (including management).”[30] This includes providing periodic security updates and implementing procedures to guard against, detect, and report malicious software (malware); monitoring login attempts and reporting discrepancies; and creating, changing, and safeguarding passwords.[31]

It is vitally important that the regulated entity adequately train management. In 2013, OCR entered into a resolution agreement and corrective action plan with Shasta Regional Medical Center after a newspaper article indicated that two senior leaders had met with media to discuss medical services provided to a patient. According to OCR’s press release, the CE impermissibly disclosed the patient’s PHI to multiple media outlets on at least three separate occasions, without obtaining a valid authorization. Former OCR Director Rodriguez admonished: “When senior level executives intentionally and repeatedly violate HIPAA by disclosing identifiable patient information, OCR will respond quickly and decisively to stop such behavior …. Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients’ rights are fully protected.”

**Conclusion**

The Security Rule requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit. This includes protecting against reasonably anticipated risks or vulnerabilities affecting confidentiality, integrity, and availability. To accomplish these goals, CEs and BAs must implement administrative, physical, and technical safeguards – including a *security management process* consisting of policies and procedures to prevent, detect, contain, and correct security violations.

Conducting a risk analysis is an important and high-profile component of the security management process. While CEs and BAs may take a flexible approach to risk analysis, it must be accurate, thorough, and enterprise-wide. Further, CEs and BAs must follow the risk analysis with a risk management plan designed to reduce risks and vulnerabilities to a reasonable and appropriate level.
The entity’s security management process must account for ePHI created, received, maintained, or transmitted on portable electronic devices. CEs and BAs must carefully consider both encryption and device and media controls to appropriately manage risk.

Risk analysis and risk management are interactive processes that grow and change with the organization and its threat environment. Neither security management component can stand alone. As this most recent resolution agreement and corrective action plan demonstrate, both are necessary (along with other security management implementation specifications) to appropriately manage risks and vulnerabilities to ePHI.

For more information on HIPAA compliance, contact Kim Metzger or a member of our Data Security and Privacy practice.

__This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.__

---

[1] 45 CFR 164.503(a)  
[5] 45 CFR 163.316(a)  
[6] 45 CFR 164.306(a)  
[7] 45 CFR 164.306(b) In deciding what security measures to use to safeguard the confidentiality, integrity, and availability of ePHI, CEs and BAs may consider their size, complexity, and capabilities; their technical infrastructure, hardware, and software security capabilities; the cost of the anticipated security measures; and the probability and criticality of potential risks to ePHI (i.e., how likely is a threat to manifest, and how serious an impact to confidentiality, integrity, and availability would results)?  
[8] 45 CFR 164.304  
[9] Id.  
[10] Id.  
[11] In August 2013, OCR announced a settlement with Affinity Health Plan, Inc., related to a breach of more than 300,000 individuals’ unencrypted ePHI stored on a leased photocopier. Affinity agreed to pay a $1.2M resolution amount, and enter into a corrective action plan, after it returned the photocopiers to leasing agents without erasing the ePHI contained on the copier hard drives. OCR’s investigation showed that Affinity failed to incorporate the ePHI stored on photocopier hard drives into its Security Rule risk analysis. Former OCR Director Leon Rodriguez commented: “This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it’s recycled, thrown away or sent back to a leasing agent. HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect this information.”  
[12] A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR 164.304)  
[14] Id.  
[15] Id.  
[16] 45 CFR 164.306(a)
“Integrity controls” are security measures to ensure ePHI is not improperly modified without detection. (45 CFR 164.312(e)(2)(i))