IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

THE UNIVERSITY OF TEXAS MD ANDERSON CANCER CENTER, Petitioner, v. UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS Respondent.	§ § § § § § § § § § § § §	Petition for Review

PETITION FOR REVIEW

Petitioner, The University of Texas MD Anderson Cancer Center, petitions this Court for review in its entirety of Decision No. 2927 of the Department of Health and Human Services, Departmental Appeals Board, Appeals Division ("DAB") entered on February 8, 2019 in DAB Case No. A-18-87 ("DAB Decision"), and which affirms Decision No. CR5111 of the Administrative Law Judge. A copy of the DAB Decision is attached.

Date: April 8, 2019

Respectfully submitted,

s/ B. Scott McBride

B. Scott McBride
State Bar No. (TX): 24002554
John W. Petrelli
State Bar No. (TX): 24056125
Morgan, Lewis & Bockius LLP

1000 Louisiana Street
Suite 4000
Houston, TX 77002-5005
Telephone: 713.890.5744
Facsimile: 713.890.5001
scott.mcbride@morganlewis.com
john.petrelli@morganlewis.com

David B. Salmons
State Bar No. (DC): 476299
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Avenue, NW
Washington, DC 20004-2541
Telephone: 202.739.3000
Facsimile: 202.739.3001
david.salmons@morganlewis.com

Counsel for Petitioner The University of Texas M.D. Anderson Cancer Center

CERTIFICATE OF SERVICE

I certify that, in accordance with Fed. R. App. P. 15(c), on April 8, 2019, I provided the clerk for the Fifth Circuit Court of Appeals with sufficient copies of this Petition for Review via the Court's ECF filing system, so that the clerk may serve Respondent with a copy of this petition. I further certify that on April 8, 2019, a true and correct copy of the foregoing Petition for Review, with attachment, was served by certified mail, return receipt requested, on Respondent's counsel listed below. There are no known additional parties to this proceeding and no additional parties that participated in the agency proceedings.

Daniel R. Wolfe
Roger C. Geer
Assistant Regional Counsels – Civil Rights Division
HHS/OGC–Region VI
1301 Young Street, Suite 1138
Dallas, Texas 75202

John F. Benevelli
Amita A. Sanghvi
Attorney Advisors
Office of the General Counsel - Civil Rights Division
330 Independence Ave. SW
Room 4647, Cohen Bldg.
Washington, D.C. 20201

s/ B. Scott McBride
B. Scott McBride

Department of Health and Human Services
DEPARTMENTAL APPEALS BOARD
Appellate Division

The University of Texas MD Anderson Cancer Center
Docket No. A-18-87
Decision No. 2927
February 8, 2019

DECISION

The University of Texas MD Anderson Cancer Center (MDA, Respondent) appeals the decision of an Administrative Law Judge (ALJ) granting summary judgment to the Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS) and sustaining civil money penalties totaling $4,348,000 under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for violating regulations requiring that health care providers implement measures to safeguard the confidentiality of protected health information and not disclose such information except as permitted by law. *The University of Texas MD Anderson Cancer Center*, DAB CR5111 (2018) (ALJ Decision). The ALJ determined that undisputed facts showed MDA violated these requirements by failing to timely implement plans to encrypt portable electronic devices. As a result, unencrypted health information of over 34,000 individuals was unlawfully disclosed when a laptop computer and two thumb drives in possession of MDA staff were stolen or lost in 2011 and 2012.

MDA argues that the ALJ erred in granting summary judgment because MDA implemented adequate safeguards and did not disclose health information in violation of the regulations and that the penalties the ALJ affirmed are excessive. We conclude that MDA identified no error in the ALJ Decision, and that undisputed evidence shows that MDA was required to encrypt its portable electronic devices containing protected health information but failed to timely do so and, thus, was liable under the HIPAA regulations for disclosures of such protected information. We affirm the ALJ Decision and the penalties the ALJ affirmed.

Legal background

The Social Security Act (Act), as amended by HIPAA and subsequently, requires a "health plan," "health care clearinghouse," or "health care provider who transmits any health information in electronic form" in connection with providing and billing for health care, to protect the privacy and security of electronic health information, and provides substantial civil money penalties (CMPs) and criminal penalties for violations of those

requirements. *See* Act, Title 11, Part C, "Administrative Simplification," §§ 1171-1180; the regulations refer to the institutions subject to these requirements as "covered entities." 45 C.F.R. § 160.103.[1]

As relevant here, section 1173(d)(2) of the Act, "Security Standards for Health Information – Safeguards" (42 U.S.C. § 1320d-1(d)(2)) requires that any covered entity "who maintains or transmits health information shall"–

> maintain reasonable and appropriate administrative, technical, and physical safeguards—
> (A) to ensure the integrity and confidentiality of the information;
> (B) to protect against any reasonably anticipated—
> (i) threats or hazards to the security or integrity of the information; and
> (ii) unauthorized uses or disclosures of the information; and
> (C) otherwise to ensure compliance with this part by the officers and employees of such person.

Section 1176 of the Act (42 U.S.C. § 1320d-5) directs the Secretary of HHS to impose CMPs "on any person who violates a provision of" these requirements, penalty amounts ranging from $100 to $50,000 for "each such violation," depending on the degree of the violator's culpability and knowledge of the violation; the section also caps the total amount that may be imposed "for all such violations of an identical requirement or prohibition during a calendar year" at amounts up to $1,500,000. Act § 1176(a).

The Secretary, as directed by HIPAA, has issued regulations implementing these provisions, with requirements for protecting the security and privacy of health information at 45 C.F.R. Part 164 and provisions for imposing and appealing CMPs at Part 160. The Part 164 regulations specify "Security Standards for the Protection of Electronic Protected Health Information," comprising "Administrative safeguards," "Physical safeguards," "Technical safeguards," "Organizational requirements" and "Policies and procedures and documentation requirements."[2] 45 C.F.R. Part 164, subpart

---

[1] The current version of the Social Security Act can be found at http://www.socialsecurity.gov/OP_Home/ssact/ssact.htm. Each section of the Act on that website contains a reference to the corresponding United States Code chapter and section. Also, a cross-reference table for the Act and the United States Code can be found at https://www.ssa.gov/OP_Home/comp2/G-APP-H.html.

[2] "Electronic protected health information," or ePHI, is protected health information "that is . . . [t]ransmitted by [or] [m]aintained in electronic media," and "protected health information," or PHI, "means individually identifiable health information . . . transmitted or maintained in any . . . form or medium," with exceptions not relevant here. 45 C.F.R. § 160.103. While HIPAA protects all PHI, we use the term ePHI when referring to the health information here as there is no dispute that the PHI at issue was maintained in electronic media.

C (§§ 164.306-164.318). These regulations are called the "Security Rule." *See, e.g*, 75 Fed. Reg. 40,868, 40,881 (July 14, 2010). In general, the Security Rule requires that "[c]overed entities and business associates must do the following:"

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
> (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
> (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
> (4) Ensure compliance with this subpart by its workforce.

45 C.F.R. § 164.306(a). Covered entities were required to comply with the HIPAA Security Rule by April 20, 2005. 45 C.F.R. § 164.318(c).

The security standards specify measures that covered entities must implement to protect health information (called "required implementation specifications"), and others they must implement if "reasonable and appropriate" (called "addressable implementation specifications"). 45 C.F.R. § 164.306(d). If a covered entity can document why an addressable implementation specification "would not be reasonable and appropriate," it must then "[i]mplement an equivalent alternative measure if reasonable and appropriate." *Id*.

As relevant here, section 164.312 of the regulations, "Technical safeguards," requires the implementation of specified standards including "access control" at section 164.312(a), which requires covered entities to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" to access the information. Section 164.312(a)(2) then lists four implementation specifications including "Encryption and decryption (Addressable)," at 45 C.F.R. § 164.312(a)(2)(iv).[3] That specification states that a "covered entity or business associate must . . . [i]mplement a mechanism to encrypt and decrypt electronic protected health information." "*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *Id*. § 164.304.

[3] The other implementation specifications for access control at section 164.312(a)(2) are "*Unique user identification (Required)*," "*Emergency access procedure (Required)*" and "*Automatic logoff (Addressable)*." 45 C.F.R. § 164.312(a)(2)(i)-(iii).

The other HIPAA requirements at issue here are the rules for the "Privacy of Individually Identifiable Health Information" in Part 164, subpart E (§§ 164.500–164.534); these requirements are called the "Privacy Rule." *See, e.g*, 75 Fed. Reg. at 40,868. Section 164.502, "Uses and disclosures of protected health information: General rules," states that "[a] covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter." 45 C.F.R. § 164.502(a).[4]

The CMP regulations at Part 160, subpart D state that "the Secretary will impose a civil money penalty on a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision" (the requirements of Part C of Title 11 of the Act). 45 C.F.R. § 160.402(a). The regulations provide tiers of per-violation penalty ranges that increase based on the violator's culpability and the extent and timing of corrective actions, if any. Culpability ranges from situations where the covered entity "did not know and, by exercising reasonable diligence, would not have known" of the violation, to situations in which the violation was due to "reasonable cause and not to willful neglect," to situations involving "willful neglect." *Id*. § 160.408. "Reasonable cause" means "an act or omission in which a covered entity . . . knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity . . . did not act with willful neglect." *Id*. § 160.401. "In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision." *Id*. § 160.406.

"In determining the amount of any civil money penalty," the regulations provide for consideration of specific factors that "may be mitigating or aggravating as appropriate." *Id*. § 160.408. Those factors are: "nature and extent of the violation," including the number of individuals affected and the time frame involved; the nature and extent of any resulting harm; the covered entity's history of noncompliance; the "financial condition of the covered entity;" and "[s]uch other matters as justice may require."

To impose a penalty, the Secretary sends the "respondent" a "notice of proposed determination" that states the legal basis for the penalty and its amount, the findings of fact regarding the violations alleged and why they warrant a penalty, the factors in section 160.408 that were considered in determining the penalty amount, and how to request an ALJ hearing to appeal the penalty. *Id*. §§ 160.420(a), 160.103. The ALJ conducts a hearing on the record but may decide cases in whole or in part by summary

[4] Permitted uses and disclosures of protected health information include disclosures to the individual who is the subject of the information and for "treatment, payment, or health care operations," as permitted elsewhere in Part 164. 45 C.F.R. § 164.502. MDA here disputes that it disclosed health information in violation of the regulations but does not argue that the alleged disclosures were permissible under the regulation.

judgment upon motion of a party "where there is no disputed issue of material fact." *Id*. §§ 160.508, 160.534. A summary judgment decision constitutes a hearing on the record for the purposes of this subpart. *Id*. § 160.508(b)(13). The ALJ "may affirm, increase, or reduce the penalties imposed by the Secretary." *Id*. § 160.546(b). The ALJ "[m]ay not find invalid or refuse to follow Federal statutes, regulations, or Secretarial delegations of authority and must give deference to published guidance to the extent not inconsistent with statute or regulation." *Id*. § 160.508(c)(1).

Before the ALJ, "[t]he respondent has the burden of going forward and the burden of persuasion with respect to any . . . [a]ffirmative defense[,] [c]hallenge to the amount of a proposed penalty . . . including any factors raised as mitigating factors[,]" any "claim that a proposed penalty should be reduced or waived[,]" and "[c]ompliance with" the requirements in the HIPAA security and privacy regulations. *Id*. § 160.534(b)(1). OCR "has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty." *Id*. § 160.534(b)(2).

Any party to the ALJ hearing may appeal the ALJ's decision to the Board, which "may decline to review the case, or may affirm, increase, reduce, reverse or remand any penalty determined by the ALJ." *Id*. § 160.548.

Case background[5]

On March 24, 2017 OCR served MDA with a Notice of Proposed Determination proposing a $4,348,000 CMP against MDA under 42 U.S.C. § 1320d-5 (Act § 1176) and 45 C.F.R. Part 160, subpart D. OCR alleged three incidents of disclosure of ePHI of at least 34,883 individuals in 2012 and 2013. The first incident was the theft of an MDA laptop computer containing PHI for 29,021 individuals from the home of an MDA physician and faculty member on April 30, 2012. The second was an MDA summer intern's loss, sometime around July 13, 2012, and possibly on an MDA employee shuttle bus, of an MDA USB "thumb drive" containing ePHI for 2,264 individuals; MDA determined that the intern's supervisor had permitted her to take the thumb drive home, contrary to MDA policy. The third incident was a visiting researcher's loss, sometime around November 27 to December 2, 2013, of a personally-owned thumb drive

[5] This background information is gleaned from the ALJ Decision, the parties' pleadings, and the record before the ALJ.

containing ePHI for 3,598 individuals; the researcher left the thumb drive on her desk and could not find it later. ALJ Decision at 7-8; MDA Request for Hearing (RFH) at 3-5; OCR Exhibits (Exs.) 56, 58, 63, 73. MDA does not dispute that it had not encrypted either the three devices or the data on them. Nor did MDA recover any of the three devices. MDA does not dispute the occurrence of the incidents, which it reported to OCR and investigated.

OCR alleged that MDA violated the regulations forbidding unauthorized disclosure of ePHI (45 C.F.R. § 164.502(a)) and requiring implementation of technical safeguards including, when reasonable and appropriate, the encryption of ePHI (45 C.F.R. § 164.312(a)(iv). For the unauthorized disclosure of ePHI resulting from the three incidents of loss of devices OCR proposed penalties of $1,000 per individual affected by each of the three incidents, resulting in the maximum annual penalties of $1,500,000 per year for 2012 and 2013 ($3,000,000 total). For the failure to comply with the technical safeguards regulation by encrypting devices including laptops and thumb drives, OCR proposed penalties of $2,000 per day for the period of March 24, 2012, through January 25, 2013 ($1,348,000 total).

MDA requested an ALJ hearing. In response, OCR filed a combined motion for summary judgment and pre-hearing brief ("OCR Brief" (Br.)), 10 attachments comprising "HHS Published Guidance," and 85 proposed exhibits. MDA filed a combined response, cross-motion for summary judgment and pre-hearing brief, and 80 proposed exhibits (R. Exs.); OCR filed a reply brief (OCR Reply); and MDA filed a surreply.[6]

Before the ALJ, OCR argued it was entitled to summary judgment because undisputed facts showed that MDA had determined to encrypt ePHI on all portable computers and devices but delayed doing so resulting in the loss of unencrypted ePHI in the three incidents, and that the proposed penalties were consistent with the regulations. MDA argued that the regulations do not require encryption and that undisputed facts show that it complied with the regulations and employed other effective measures to protect ePHI, that three incidents were the fault of staff who acted in defiance of MDA policies in which they had been trained, and that the proposed CMPs were excessive. MDA also argued that the regulations exceeded statutory authority by subjecting government entities to HIPAA enforcement and imposing excessive penalties, and that the CMPs that MDA proposed were unconstitutionally excessive.

[6] We use and abbreviate the terms the ALJ used to identify the parties' briefing.

The ALJ Decision

The ALJ concluded that "undisputed material facts establish that Petitioner failed to comply with" the two regulations OCR charged it with violating. ALJ Decision at 5. The ALJ first concluded that MDA violated the technical safeguards/access control regulation at section 164.312(a)(2) because it was "aware of the need to encrypt devices in order to assure that confidential data including ePHI not be improperly disclosed," selected encryption of devices as "its primary protective mechanism," and "established a policy requiring the encryption and protection of devices containing ePHI," but "made only half-hearted and incomplete efforts at encryption over the ensuing years" and thus "failed to activate that mechanism." *Id*. at 5, 7. This failure, the ALJ concluded, led to "the unlawful disclosure of ePHI relating to tens of thousands of Respondent's patients" in the theft of the laptop in April 2012 and the loss of the two thumb drives in July 2012 and November/December 2013. *Id*. at 5. The ALJ cited, as examples of these undisputed facts, information security policy issuances from MDA and the University of Texas, and MDA documents including institutional reports, project summaries, training materials, internal correspondence, and correspondence with OCR. ALJ Decision at 5-7. The ALJ rejected MDA's arguments that encryption is optional and that the regulation does not require encryption of electronic devices (as opposed to files), explaining that MDA had determined to rely on encryption of portable electronic devices but delayed doing so. *Id*. at 7, 9.

The ALJ also concluded that these undisputed facts and the three incidents of theft and loss demonstrated that MDA violated the Privacy Rule prohibition against unauthorized disclosure of ePHI at 45 C.F.R. § 164.502(a). *Id*. at 9-12. The ALJ ultimately concluded that MDA "recognized a problem, consisting of the vulnerability of its ePHI to unauthorized disclosure including by loss or theft, devised a mechanism to protect ePHI that included encryption of devices, and failed to implement that mechanism." *Id*. at 12.

Next, the ALJ concluded that the proposed CMP amounts were reasonable under the regulatory factors, and sustained OCR's application of the "reasonable cause" culpability level. *Id.* at 12-17. The ALJ also concluded he had no authority to address MDA's arguments that the regulations were in conflict with the statute or permitted penalties that were unconstitutionally excessive.

We address the ALJ Decision in greater detail in our analysis below.

Standard of Review

Whether summary judgment is appropriate is a legal issue the Board addresses de novo, viewing the proffered evidence in the light most favorable to the non-moving party. *Timothy Wayne Hensley*, DAB No. 2044, at 2 (2006). Summary judgment is appropriate if there is no genuine dispute of fact material to the result and the moving party is entitled to judgment as a matter of law. *See 1866ICPayday.com, L.L.C.*, DAB No. 2289, at 2 (2009) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-25 (1986)); *Everett Rehab. & Med. Ctr.*, DAB No. 1628, at 3 (1997) (citing *Travers v. Shalala*, 20 F.3d 993, 998 (9th Cir. 1994)). In examining the evidence to determine the appropriateness of summary judgment, an ALJ must draw all reasonable inferences in the light most favorable to the non-moving party. *See Brightview Care Ctr.*, DAB No. 2132, at 2, 9 (2007); *but see Cedar Lake Nursing Home*, DAB No. 2344, at 7 (2010); *Brightview* at 10 (entry of summary judgment upheld where inferences and views of nonmoving party are not reasonable). Drawing factual inferences in the light most favorable to the non-moving party does not require that an ALJ accept the non-moving party's legal conclusions. *Cedar Lake Nursing Home* at 7.

"The standard of review on a disputed issue of law is whether the decision is erroneous." 45 C.F.R. § 160.548(h).

Analysis

As an initial matter, we note that MDA has devoted much of its appeals – to the ALJ and the Board – to advancing arguments that seek relief that neither we nor the ALJ may grant. MDA has admitted it is a "covered entity" within the meaning of the HIPPA regulations. RFH at 3; *see also* 45 C.F.R. § 160.103 (defining "covered entity" to include a "health plan," a "health care clearinghouse," and a "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."). Nonetheless, MDA argues that the applicable regulations are invalid as ultra vires the statute. More specifically, MDA argues: 1) that as "an agency of the State of Texas" it is not subject to HIPAA enforcement because the Act imposes penalties on a "person," which the regulations, but not the Act, define as including public entities; 2) that the maximum yearly penalties the regulations permit for MDA's level of culpability exceed those in the Act; and 3) that the CMPs imposed "are excessive in violation of the Eighth Amendment of the U.S. Constitution." NA at 3-9, 26-28, 32-34.

The ALJ correctly ruled that he "ha[s] no authority to address" these arguments because he has no authority "to find that the Secretary's regulations are ultra vires" or "to declare unconstitutional proposed actions by agencies of this Department." ALJ Decision at 3. The ALJ did not err. The HIPPA appeal regulations themselves state that the ALJ "[m]ay not find invalid or refuse to follow Federal statutes, ***regulations***, or Secretarial

delegations of authority." 45 C.F.R. § 160.508(c)(1) (emphasis added). The ALJ thus did not err in declining to grant MDA relief based on its arguments that the regulations are ultra vires or otherwise invalid. In addition, in reviewing ALJ decisions in appeals of penalties imposed by other HHS agencies on entities (e.g. nursing facilities, health care providers and suppliers) for violations of other regulations, the Board has held that a duly-issued regulation "is binding on the agency that issues it" and that it is "well established that administrative forums, such as this Board and the Department's ALJs, do not have the authority to ignore unambiguous statues ***or regulations*** on the basis that they are unconstitutional." *Hermina Traeye Mem'l Nursing Home*, DAB No. 1810, at 21 (2002), *aff'd*, *Sea Island Comprehensive Healthcare Corp. v. U.S. Dep't of Health & Human Servs.*, 79 F. App'x 563 (4th Cir. 2003), (citing *Sentinel Med. Labs*., *Inc.*, DAB No. 1762, at 9 (2001), *aff'd*, *Teitelbaum v. Health Care Fin. Admin.*, 32 F. App'x 865 (9th Cir. 2002)). As the Board stated in *Central Kansas Cancer Institute*, DAB No. 2749, at 10 (2016), an appellant "is free to make [its] *ultra vires* argument to a court, but we may not invalidate a regulation." We accordingly do not address these arguments asking us to ignore or declare regulations invalid, and move on to address MDA's other arguments.

I. The ALJ's conclusion that MDA violated the requirements of 45 C.F.R. § 164.312(a) by failing to complete the encryption of its portable electronic devices is legally correct.

A. MDA was required to implement encryption.

MDA argues that its failure to timely encrypt portable electronic devices did not violate the Security Rule because section 164.312(a)(2)(iv) designates encryption as "addressable" and thus, according to MDA, optional. *See* MDA Notice of Appeal & Brief (NA Br.) at 3 (MDA "was not required to implement an optional ("addressable") device-level encryption specification"). MDA cites section 164.306(b), "Flexibility of approach," stating that covered entities "may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." *Id*. at 11. MDA also cites language from the preamble to the notice of final rulemaking revising Part 164 that acknowledges "greater flexibility in satisfaction of the requirements" and states that for "addressable specifications, an entity decides whether each specification is a reasonable and appropriate security measure to apply within its particular security framework." *Id*. at 11-12 (citing 68 Fed. Reg. 8334, 8364, 8369 (Feb. 20, 2003)). MDA also notes that the encryption regulation is one of four "implementation specifications" for meeting the "access control" standard at section 164.312(a) (and one of two addressable specifications), and argues that "reading the regulations in their context, it is clear that [MDA] was permitted to 'address' the nonrequired 'encryption and decryption' implementation specification with 'any security measures' that were 'reasonable and appropriate' to establish a mechanism for encryption and decryption of ePHI." *Id*. at 12.

These arguments misstate the law. As discussed below, the regulations require encryption to protect the privacy of personal medical information and prevent its unlawful disclosure unless the covered entity documents that encryption is not "reasonable and appropriate" but that some alternative measure is. Undisputed evidence shows that MDA did not determine that encryption was not reasonable and appropriate but, on the contrary, determined that encryption, and specifically electronic device encryption, was reasonable and appropriate. Thus, as we discuss later, its evidence of alternative measures is not material.

1. *The regulations require encryption absent a determination it is not a reasonable and appropriate mechanism for protecting ePHI.*

MDA's "optional" argument misstates the addressable implementation specifications and ignores language in section 164.306 imposing conditions on an entity's ability to decline to implement addressable implementation. Section 164.312(a)(2)(iv) states that a covered entity "***must*** . . . [i]mplement a mechanism to encrypt and decrypt electronic protected health information" (emphasis added). This is plainly mandatory. While explanatory language in section 164.306(d) distinguishes addressable and required implementation specifications and incorporates a "reasonable and appropriate" element in the requirement to implement addressable specifications, that language does not describe "addressable" requirements as "optional" and explains the obligations entailed by the term "addressable":

> (3) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity or business associate must—
>
> (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
>
> (ii) As applicable to the covered entity or business associate—
>
> (A) Implement the implementation specification if reasonable and appropriate; or
>
> (B) If implementing the implementation specification is not reasonable and appropriate—
>
> (*1)* Document why it would not be reasonable and appropriate to implement the implementation specification; and
>
> (*2)* Implement an equivalent alternative measure if reasonable and appropriate.

45 C.F.R. § 164.306(d). The Secretary explained in the preamble to the final notice adopting the CMP rules at Part 164 the obligations incumbent on an entity that elects not to implement an addressable specification. In response to a question about how the term "violation . . . would apply to the addressable implementation specifications of the Security Rule," the preamble states:

> **[A] covered entity must implement an addressable implementation specification if doing so is "reasonable and appropriate."** Where that condition is met, the addressable implementation specification is a requirement, and failure to implement the addressable implementation specification would, accordingly, constitute a violation. **Where that condition is not met, the covered entity must document why it would not be reasonable and appropriate to implement the implementation specification and implement "an equivalent alternative measure if reasonable and appropriate."** In this latter situation, creating the documentation referred to is a requirement, and implementing an alternative measure is also a requirement, if doing so is reasonable and appropriate in the covered entity's circumstances; failure to take either required action would, accordingly, constitute a violation.

71 Fed. Reg. 8390, 8393 (Feb. 16, 2006) (emphasis added). OCR similarly explained that addressable implementation specifications were not optional in guidance published in 2010 addressing the required "risk analysis" implementation specification at section 164.308(a).[7] In that guidance, OCR explained that the Security Rule (Part 164, subpart C)–

> contains several implementation specifications that are labeled "addressable" rather than "required." (68 FR 8334, 8336 (Feb. 20, 2003).) **An addressable implementation specification is not optional**; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so. (See 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306(d)(3).)

[7] The "*Risk analysis (required)*" specification states that a covered entity must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate." 45 C.F.R. § 164.308(a)(1)(ii)(A).

> The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Organizations should use the information gleaned from their risk analysis as they, for example:
>
> * * *
>
> - Decide whether and how to use encryption. . . .

Guidance on Risk Analysis Requirements under the HIPAA Security Rule at 3 (July 14, 2010) (OCR Br. Att. 3) (emphasis added).[8]

This preamble and guidance language confirms that, consistent with the regulation, a covered entity such as MDA **must** implement an addressable specification such as encryption **unless** the covered entity makes a determination that encryption is not "a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information," and documents that determination.[9] As we discuss next, undisputed evidence shows that MDA did not determine or document that encryption was not reasonable and appropriate. On the contrary, as discussed below, the undisputed facts show that MDA determined encryption – and specifically through the mechanism of encrypting its portable electronic devices – was reasonable and appropriate.

2. *Undisputed evidence shows that MDA determined that encryption of its portable electronic devices was reasonable and appropriate and made no contrary determination.*

MDA does not deny having determined that encryption was "a reasonable and appropriate safeguard" to protect ePHI and does not allege that it determined, and documented, that encryption was not reasonable and appropriate. This is apparent from unchallenged MDA documents showing, as the ALJ concluded, that MDA was aware of the risk of loss of ePHI in theft or loss of portable electronic devices and determined to encrypt those devices to protect against that risk.

---

[8] Available at https://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html.

[9] An ALJ "must give deference to published guidance to the extent not inconsistent with statute or regulation"; this restriction applies to the Board. 45 C.F.R. § 160.508(c)(1); 71 Fed. Reg. at 8416 ("[W]e require ALJs and the Board to follow guidance which has been publicly disseminated, unless the ALJ or Board finds the guidance to be inconsistent with statute or regulation."). As explained above, the guidance's explanation of the conditions prerequisite to not implementing an addressable implementation specification are consistent with the regulations.

The ALJ found that MDA "knew that its ePHI was subject to exposure through disclosure, including inadvertent disclosure, through data loss or theft" following the 2005 theft of "a laptop containing information of about 4000 [MDA] patients." ALJ Decision at 13. The ALJ also found that the University of Texas advised MDA in 2007 "that many incidents involving unauthorized exposure of confidential data result from theft or loss of portable devices that contain such data," and that also in 2007 MDA "identified mobile media data security as a high level risk." *Id*. at 6. As late as June 2013, the ALJ found, an MDA risk analysis identified failure to encrypt data as a high risk impact area. *Id*. at 7.

The evidence the ALJ cited included a University of Texas Security Bulletin from June 1, 2007 (OCR Ex. 2), an MDA Institutional Compliance Quarterly Report from September 2007 stating that "Mobile Media Security" was classified as being at a high risk level (vs. low and medium) (OCR Ex. 26, at 4), and an MDA "FY 2013 Institutional Compliance Office Annual Risk Analysis" dated June 12, 2013, that identified "[f]ailure to encrypt data at rest within information systems" and "[f]ailure to prevent unauthorized downloading of ePHI, Confidential, and Restricted Confidential Information onto portable computing devices" as "high probability, high impact" "risk areas" (OCR Ex. 22, at 2). *Id*. at 6-7.

To address those identified risks, the ALJ found it undisputed that, beginning as early as 2006, MDA "consistently stated that confidential data, including ePHI, must be protected against loss or theft"; "repeatedly announced a policy that both required encryption of confidential data and prohibited unsecured storage of such data"; "often reiterated its policies concerning protection and non-disclosure of confidential information including ePHI"; and "eventually determined that the mechanism with which it would protect confidential data including ePHI would be the encryption of the devices on which such data is stored." *Id*. at 5, 6.

The ALJ cited MDA's 2006 Information Resources Security Operations Manual, which "explicitly require[d] that data stored on media, including transportable media and laptops, that travel from Respondent's premises must be encrypted or protected with access controls"; prohibited MDA staff from "unauthorized removal of devices containing confidential data"; and "direct[ed] that such data stored on transportable media must be encrypted." ALJ Decision at 5 (citing OCR Ex. 1, at 3, 24, 26, 29). The ALJ also cited MDA's "Information Security Program and Annual Report" for 2008, prepared by MDA's director of information security, stating that among the initiative MDA "plans to undertake" in 2009, was to "[i]mplement the first phase of a Media Security Project, which will test and implement encryption on institutional laptops and desktops so MDACC data remains protected if a system is lost or stolen." OCR Ex. 9, at

10; *see* ALJ Decision at 6. The same report for 2010 states that MDA "continues work on addressing key risk areas that are currently not mitigated, such as encryption of confidential data on mobile media," including work to "complete the Analysis and Planning phase" of a "Media Encryption for Laptops and Desktops Project." OCR Ex. 11, at 11; *see* ALJ Decision at 6.

In addition, the ALJ cited a "Risk Analysis Ranking Tool" from February 2011 that again identified "[l]ack of encryption for portable computing devices" as a "high probability, high impact" "risk area" and stated that vendors were being selected for the "Encryption for Desktops and Laptops Project" and that "[t]he Encryption Project is being initiated"; and MDA emails indicating that MDA in September 2012 purchased and began distributing "IronKey" encrypted USB drives to staff. OCR Exs. 14, at 3; 47; 48; *see* ALJ Decision at 6, 7. The ALJ also cited a June 2012 memo from the university executive vice chancellor for health affairs on the subject "**Highest Priority- Encryption of all University Laptop Computers,**" noting that since 2007, the university had "avoided a number of serious data exposures due to laptop computers having been encrypted prior to becoming lost or stolen" but had "experienced incidents in which encryption of laptops had not been put in place," some of which "resulted in serious data exposures," and advising that "[**o**]**ur real-world experience teaches us that laptop encryption cannot be optional**" and "**must be a required security control for all University laptop computers,**" and stating a "**target for encryption is 100% of these computers by August 31, 2012**." OCR Ex. 41, at 1 (emphasis added); *see* ALJ Decision at 7.

MDA does not dispute the ALJ's descriptions of these exhibits, which were all documents issued by MDA (or its parent university in one instance), and does not argue that the ALJ misconstrued their contents or drew inferences from them to the detriment of MDA's case.

Moreover, additional documents in the record, some of which OCR cited in moving for summary judgment and in response to MDA's appeal of the ALJ Decision, further confirm that MDA determined that electronic device encryption was "reasonable and appropriate" to safeguard ePHI maintained on portable computing devices. We consider all of these exhibits, which comprise materials generated by MDA, as part of our de novo review. These include an August 2011 presentation on the status of MDA's project to encrypt laptops and desktops, with a timetable projecting "mass deployment" during May through August 2012 (OCR Ex. 33, at 3); a September 2011 MDA presentation on encryption to the faculty senate that noted examples of breaches due to stolen laptops and stated plans to "[e]nable portable media encryption (CDs & thumbs drives)"to be

completed by August 2012 (OCR Ex. 35, at 3, 5), and the Information Security Program and Annual Report for 2011, stating that MDA had "[i]dentified and acquired a solution to encrypt institutional laptops and desktops" and had completed "the implementation of the supporting infrastructure with the goal of encrypting all laptops and desktops by the end of FY12" (OCR Ex. 13, at 4, 8).

In addition, MDA reported to OCR in a letter dated January 25, 2013, which cited an internal email on June 12, 2012 from "Integrated Technology Services . . . discussing 'surge' initiative," that "the President's office has directed that the encryption of computers, especially laptops, be significantly accelerated" and that "ALL laptops must be encrypted within the next 72- 90 hours." R. Ex. 51, at 27. The letter references other internal MDA emails "discussing prioritization of encryption process" and "acceleration of efforts to encrypt all [MDA] computers." *Id*.

Finally, a September 2012 presentation by the MDA Institutional Compliance Office, "IronKey Distribution Event: Why We're Doing What We're Doing," noted the "recent events" of the theft of the unencrypted laptop and the unencrypted USB flash drive; the requirement to "[i]mplement a mechanism to encrypt and decrypt" ePHI "[w]here it is a reasonable and appropriate safeguard for a covered entity"; the "potential for fines (Alaska Medicaid fined $1.7 million)"; and stated that "[**i**]**t's reasonable and appropriate for** [**MDA**] **to encrypt thumb drives**." OCR Ex. 49, at 1-2 (emphasis added).

These documents, and those the ALJ cited, show that MDA required data encryption by at least 2008 or 2009, committed itself around that time to encrypt all portable computers and maintained that objective over the coming years, and later determined to require the use of encrypted flash or thumb drives. These documents reflect a considered, ongoing determination that encryption of its portable electronic devices was the principal means by which it would safeguard ePHI on those devices, and they establish that MDA determined that this encryption was a reasonable and appropriate safeguard.

MDA does not deny that it determined to encrypt its portable electronic devices as the exhibits evidence; nor does MDA assert that it determined that encryption was not a reasonable and appropriate safeguard. Indeed, MDA appears to agree that its records establish that it selected encryption of its devices to safeguard confidential data, as it accused the ALJ of "seizing upon [MDA's] internal effort to *improve its security mechanisms* by establishing a practice of encrypting devices" based "on the internal, self-critical risk assessments voluntarily furnished by [MDA] to the OCR." NA Br. at 15 (MDA's italics).

The Security Rule thus required that MDA implement the encryption mechanism that, over a period of years, it planned and committed itself to implement. As we explain next, undisputed evidence shows that it did not.

B. Undisputed evidence shows that MDA did not implement encryption of its portable electronic devices as required.

The ALJ held that MDA did not comply with the encryption requirement because "despite identifying the risk of and dangers related to confidential data loss and deciding on encryption of devices as a means of protecting such data," MDA "delayed for years implementing its self-selected mechanism for protecting ePHI, encryption of portable devices" and then proceeded "at a snail's pace," resulting in "ePHI pertaining to more than 33,000 individuals being lost or stolen in 2012 and 2013." ALJ Decision at 6, 9.

The ALJ found that undisputed evidence showed that MDA put its encryption efforts "on hold due to financial constraints" in 2009, when "it had not encrypted any of the several thousand laptops that it controlled," and that as of August 2011, MDA "had not commenced laptop encryption . . . despite its continued recognition that lack of encryption put its confidential data at high risk." *Id*. at 6 (citing OCR Exs. 10, at 6; 11, at 11, 13, 15; 14; 27, at 1, 4). MDA "finally" began "mass encryption of its laptops" in May 2012, but as of November 2013, "more than ten percent of its computers ["[m]ore than 4400"] remained unencrypted," despite the university's goal of encrypting all laptop computers by August 31, 2012. *Id*. at 7 (citing OCR Exs. 39, at 5; 41; 71, at 3-4). "As of January 2014," the ALJ found, "nearly ten percent of Respondent's computers – more than 2600 devices – remained unencrypted." *Id*. (citing OCR Ex. 71, at 4). MDA moreover "did not purchase and distribute encrypted USB devices ('IronKeys') until September 2012 after the loss of an unencrypted USB device." *Id*. (citing OCR Exs. 47; 48).

MDA reported in its letter to OCR dated January 25, 2013 that as of that date it "ha[d] encrypted 98% of [MDA]-managed desktop desktops and laptops, with the remaining 2% scheduled to be completed in February 2013."[10] R. Ex. 51, at 27. OCR stated in its Notice of Proposed Determination that it "[a]lthough [MDA] had yet to achieve a complete rate of encryption as required by 45 C.F.R. § 164.312(a)(2)(iv), OCR determined to end the non-compliance period for this violation on January 25, 2013 in recognition of encryption of its managed computer inventory as of that date." Notice of Proposed Determination at 4 n.2.

MDA does not dispute any of the figures or dates the ALJ cited or deny that it delayed its encryption efforts as the ALJ described. Instead, MDA argues it "did implement the 'addressable' encryption specification for the period of March 24, 2011 through January 25, 2013" with "multiple layers of security measures (including administrative, physical, and technical safeguards) that, MDA claims, constituted its "'mechanism' for addressing

[10] MDA reported that "managed" computers are "all desktops and laptops that send and receive data into one of three [Computer Management System] consoles." OCR Ex. 71, at 2.

the encryption and decryption of ePHI." NA Br. at 3, 13 (citing R. Exs. 5-39). MDA, however, cites only measures *other* than encryption of portable computers, such as "password-protected access controls," employee training, and the requirement in its Information Security Manual that users encrypt and back up on network servers confidential data stored on portable computing devices (a measure that users in the three incidents also failed to employ). *Id*. at 13-14. MDA offers no explanation that would allow the Board to reasonably infer that these other measures somehow constituted a "mechanism" for achieving encryption, or that they constituted, or were ever intended as, "an equivalent alternative measure" that was "reasonable and appropriate," as required by section 160.306(d)(3)(11)(B)(2).

The regulations, in any case, did not permit MDA to forgo encryption in favor of alternative measures, even had MDA shown them to be "equivalent," absent a documented determination of "why it would not be reasonable and appropriate to implement the implementation specification" of encryption. 45 C.F.R. § 164.306(d)(3)(ii)(B)(*1*). There is no dispute that MDA did not document having ever made that determination here. As undisputed evidence shows that MDA determined that encryption of its portable electronic devices was a reasonable and appropriate method to safeguard confidential data including ePHI, it was obliged to implement encryption of the devices, irrespective of whether it also employed other methods to protect data, as the ALJ accepted for the purpose of ruling on OCR's motion for summary judgment. As the ALJ stated,

> Encryption . . . was the mechanism that Respondent chose to protect its ePHI contained on portable devices. Once Respondent elected to utilize that mechanism, it was obligated to make it work.

ALJ Decision at 9. Moreover, while the ALJ acknowledged "[t]he approaches touted by Respondent," he found no evidence that those approaches were "intended to substitute for encryption," noting, "Respondent has pointed to no facts that suggest or establish that at some point after 2008 it decided to implement alternate mechanisms other than encryption to protect its ePHI." *Id*. The ALJ also found that, "even if Respondent adopted the various approaches in lieu of encrypting devices that it asserts were its mechanism to protect ePHI, those approaches failed spectacularly to protect Respondent's confidential data, with ePHI pertaining to more than 33,000 individuals being lost or stolen in 2012 and 2013." *Id*. We agree with the ALJ that nothing that MDA has presented supports any reasonable inferences that it ever found encryption not reasonable and appropriate for its systems or that some equivalent alternative measure(s) would be reasonable and appropriate. We also agree that any steps MDA did take proved ineffective.

In conclusion, MDA has cited no evidence raising a genuine dispute of material fact that it violated the HIPPA regulations by failing to timely implement the encryption of its portable electronic devices, the mechanism MDA repeatedly and consistently determined was reasonable and appropriate to safeguard the confidentiality of its protected health information.

C. MDA's other arguments show no error in the ALJ's conclusion that MDA violated the access control regulation at section 164.312(a)(2).

MDA argues that the ALJ failed "to view the evidence in the light most favorable to the non-moving party, drawing all reasonable inferences in that party's favor" because the ALJ declined to admit any exhibits yet "cited 23 separate OCR exhibits in support of the facts he took as 'undisputed'" but "not a single exhibit of the 80 offered" by MDA. NA Br. at 10.

OCR moved and MDA cross-moved for summary judgment. ALJ Decision at 2. OCR filed 85 proposed exhibits in support of its motion, and MDA filed 80 proposed exhibits in support of its cross-motion and opposition to OCR's motion. As the Board noted in *Illinois Knights Templar Home*, DAB No. 2274, at 6-7 (2009), while an ALJ is required to review all proposed exhibits submitted in support of or in opposition to a motion for summary judgment in order to determine whether there is a material dispute of fact precluding summary judgment, the ALJ is not required to admit those exhibits into the record in order to conduct this review and make this determination. Such exhibits, the Board stated, are "'properly treated as an offer of proof, that may be evaluated if necessary to determine whether a genuine issue of material fact exists' in considering a motion for summary judgment." *Id*. (citing *Lackawanna Med. Grp. Lab.*, DAB No. 1870, at 14 (2003) (finding no prejudice to either party where neither party specifically identified on appeal anything in the exhibits that would have made a difference to the ALJ's determination)).

That the ALJ cited only OCR exhibits is not evidence that he did not review MDA's exhibits. Moreover, we have reviewed the entire record, and find no basis for concluding that the ALJ overlooked any evidence that is material to his decision or ours.

It is important to note that, in this case, nearly all of the OCR exhibits the ALJ cited consist of documents prepared by and obtained from MDA or, in a few instances, MDA's parent university. As OCR points out, the ALJ cited only three documents that MDA did not create, consisting of two memos by an OCR specialist describing phone interviews with the researcher with the stolen laptop and with the intern who lost the thumb drive in

July 2012 (OCR Exs. 59, 64), and a printout of a February 2006 newspaper article reporting on the November 2005 theft of a laptop containing insurance claims of nearly 4,000 MDA patients (OCR Ex. 79).[11] OCR Resp. at 17; ALJ Decision at 7, 8, 13. MDA did not object to any of the OCR exhibits the ALJ cited, including the three that MDA did not create, and does not argue that the ALJ misread or improperly construed their contents against MDA.

MDA does not cite any of its exhibits that the ALJ decision does not discuss which are material to the issue before us, i.e., whether MDA failed to comply with HIPPA regulations when it did not implement a mechanism to encrypt and decrypt all its portable electronic devices containing ePHI – leading to unlawful disclosure of protected information – despite having determined that encryption was the reasonable and appropriate approach to protecting ePHI in its environment. The ALJ's citations to MDA's own documents to illustrate the absence of a dispute of fact material to this issue does not constitute error.

The exhibits MDA accuses the ALJ of ignoring were not material because they were offered to support the legally erroneous conclusion that MDA could forgo encryption in favor of other measures. As discussed above, the regulations did not permit MDA to forgo encryption because it did not document a determination that encryption was not reasonable and appropriate. Indeed, the record, as discussed above, shows no genuine dispute that MDA, in fact, determined, in its own words, not only that encryption was "reasonable and appropriate" but that encryption "must be a required security control for all University laptop computers." OCR Exs. 41, at 1; 49, at 1-2.

MDA was legally required to implement encryption, and it determined that the mechanism to fulfill that requirement was to encrypt its portable electronic devices to safeguard confidential data. Yet, MDA failed to implement that encryption in a timely manner. *See, e.g.*, R. Ex. 51, at 27 (MDA January 25, 2013 letter, cited supra, reporting plans to accelerate computer encryption and that MDA had encrypted 98% of "managed" computers).

We also note that the evidence MDA cites as having been ignored (NA at 13-14), the written testimony of its executive director and chief information security officer, is consistent with other unchallenged evidence (including evidence cited by the ALJ), in that the testimony recognizes the importance MDA put on device encryption even if, as MDA contends, it also used other means to protect ePHI. *See* R. Ex. 74, at 2, 7, 8 (stating

[11] The two interview memos cited by the ALJ confirm that MDA staff, including those in supervisory positions, did not follow MDA policies forbidding the removal from MDA premises of devices containing unencrypted confidential health information. *See* OCR Exs. 59, 64.

that "[d]evice-level encryption" was a "component of [MDA's] overall information security strategy"; that MDA "purchased 5,000 4GB IronKey hardware encrypted thumb drives" in August 2012; and describing "the cost and effort required to implement the full-disk computer encryption at [MDA]").

Finally, we find no basis for Respondent's suggestion that it was not noncompliant because "[t]he regulations do not require device-level encryption," as compared to file encryption. *See, e.g.*, NA Br. at 3. Regardless of whether the regulations require that encryption, which is mandatory, be done through encryption of devices, as compared to encryption of files, the undisputed evidence we discussed above shows that MDA deliberately selected the encryption of its devices as its means of accomplishing what the regulations require, that access to data be restricted by means of encryption. *See* ALJ Decision at 9 (encryption of devices "was the mechanism that Respondent chose to protect its ePHI contained on portable devices"). Having chosen that mechanism to meet the encryption requirement, MDA was required to fully implement it, not some other mechanism.

II. MDA has shown no error in the ALJ's conclusion that MDA disclosed ePHI in violation of section 164.502(a).

A. The three incidents constituted disclosure of PHI prohibited by section 164.502(a).

As noted above, there is no dispute that ePHI for over 34,000 individuals was lost in the theft of the laptop and the loss of the two thumb drives in 2012 and 2013. We find no error in the ALJ's determination that these three incidents were prohibited disclosures. Disclosure "means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 C.F.R. § 160.103. MDA's argument that the regulatory definition of "disclosure" does not include the loss or misplacement of the PHI stored on the stolen laptop and the two lost thumb drives ignores the plain meaning of the terms in the regulatory definition of "disclosure" and preamble guidance confirming that finding a prohibited disclosure does not require any showing that the protected information was obtained or viewed by someone outside of the covered entity.

As the ALJ noted, the common dictionary definition of "release," which is one of the regulatory meanings of disclosure, includes "to set free from restraint," which does not require "a third party recapturing that which has been released." ALJ Decision at 10 (citing https://www.merriam-webster.com/dictionary/release). Nothing in this definition or in the regulatory definition of disclosure requires that lost ePHI be read, accessed by or provided to anyone outside of the covered entity. As OCR points out, the Secretary, in

the preamble to the final rule first publishing Parts 160 and 164, advised that "[d]isclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security," which is consistent with the common sense meaning the ALJ applied. 65 Fed. Reg. 82,462, 82,467 (Dec. 28, 2000).

MDA cites a federal court decision holding, in part, that "the possibility that a record might be revealed to unauthorized readers by negligent or reckless transmission" by facsimile was not a "disclosure" prohibited by the federal Privacy Act of 1974 at 5 U.S.C. § 552a. NA Br. at 20-21 (quoting *Luster v. Vilsack*, 667 F.3d 1089 (10th Cir. 2011)). The *Luster* decision does not apply here, as it addresses provisions of the Privacy Act that: (1) require that the disclosure be "by any means of communication ***to any person***"; and (2) expressly require that the disclosure be "***intentional or willful***"; the HIPAA regulations contain neither requirement. *See* 667 F.3d at 1097 (citing *Wilkerson v. Shinseki,* 606 F.3d 1256, 1268 (10th Cir. 2010)); *see also Jacobs v. Nat'l Drug Intelligence Ctr*, 423 F.3d 512, 515-16 (5th Cir. 2005); 5 U.S.C. § 552a(b) (emphasis added) (prohibiting unexcepted disclosures "by any means of communication to any person"), (g)(4) (emphasis added) (authorizing actions for damages when the disclosure "was intentional or willful").

We also note that the regulatory definition of "disclose" includes "provision of access to," and MDA's loss of the three devices containing ePHI in unencrypted form is most reasonably viewed as providing access to whomever might acquire the lost media. We see no requirement that OCR establish that someone actually acquired the media or, if someone did, whether any such person viewed or extracted or used the data.

In short, the loss of the devices contain ePHI in a manner that did not ensure that access to the data would be restricted to those properly entitled to it amounted to a release of the ePHI and its disclosure in violation of section 164.502(a).

B. The regulations do not exempt MDA from the consequences of its disclosure of ePHI on the ground that the ePHI involved research.

MDA argues that, even if the data were disclosed, "OCR's allegations of 'disclosure' do not apply to the data at issue," arguing that research data "is not subject to HIPAA." NA at 3; *see also* at 21-22. MDA relies on the December 2000 preamble to the final rule publishing the Privacy Rule at Part 164 subpart E as stating that "'Congress did not include information created or received by a researcher' within the definition of individually identifiable health information" and that HHS "cannot apply any restrictions or requirements on a researcher . . . and protections do not apply to those research records." NA Br. at 21-22 (quoting 65 Fed. Reg. at 82,575, 82,611) (internal quotation marks omitted).

The ALJ, however, rejected MDA's claim, based on preamble language, of a HIPAA exemption for "research information" because "Respondent has identified nothing in the regulations that even ostensibly supports that argument." ALJ Decision at 11. The ALJ also agreed with OCR that the preamble language upon which MDA relied, which states that HHS "cannot apply any restrictions or requirements on a researcher . . . and protections do not apply to those research records," was "meant to apply to the very limited instance of research conducted by non-covered entities and business associates that receive information from covered entities." *Id*. (citing 65 Fed. Reg. at 82,575; OCR Reply at 10-11). The ALJ also held that "[MDA]'s argument ignores the fact that there is a regulatory mechanism for a facility to segregate its research function from its clinical function and to exempt its research function from non-disclosure requirements" and that MDA "does not argue it made any effort to do so." *Id*. The ALJ cited 45 C.F.R. § 164.105, which provides for "hybrid entit[ies]," and 65 Fed. Reg. at 82,569, stating that the Privacy Rule "gives covered entities some flexibility to segregate or aggregate [their] operations").

On appeal, MDA continues to rely on the preamble language but has not alleged any error in, or responded to, the ALJ's conclusion that the HIPAA regulations do not exempt all research data from the requirements of the HIPAA regulations. *See* 45 C.F.R. § 160.548(c) ("A notice of appeal must be accompanied by a written brief ***specifying exceptions to the initial decision and reasons supporting the exceptions***." (emphasis added)). In particular, MDA did not respond to the ALJ's agreement with OCR that the preamble language concerned research conducted by non-covered entities and that MDA did not allege that it sought to segregate its research and clinical (i.e., covered entity) components. ALJ Decision at 11; OCR Reply at 10-11. We also note that, while the regulations permit ePHI to be used in research under specified conditions, they do not indicate that the ePHI is thereby rendered exempt from the prohibitions on unauthorized disclosure. *See* 45 C.F.R. § 164.512(i). MDA does not argue that it met the conditions for using ePHI in research, or that it was a "hybrid entity" with a research component segregated from its clinical component

The ALJ thus did not err in concluding that there was no merit to MDA's argument that it was exempt from HIPAA enforcement on the ground that the ePHI it disclosed was research information. ALJ Decision at 11.

C. The ALJ did not err in holding MDA liable for the loss of ePHI in the three incidents.

The ALJ rejected MDA's argument that it was not liable for the actions of its employees in the three incidents because they acted contrary to MDA policy by taking devices with unencrypted ePHI off premises. *Id*. at 12; NA Br. at 4 ("[T]he unsanctioned actions of employees acting against the company cannot be imputed to the company."). As the ALJ noted, "[u]nder HIPAA a principal is liable for the acts of its agents, including its

employees, who act within the scope of their duties." The ALJ cited 45 C.F.R. § 160.402(c), which states at paragraph (c)(1) that "[a] covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency."

MDA argues as below that staff in the three incidents were "acting outside of their scope of agency" and cites the preamble to a 2013 final rule revising Parts 160 and 164, which it says "explained that the section [160.402(c)] 'does not make a covered entity liable for the acts of third parties that are not under its control . . . .'" NA Br. at 22-23 (citing 78 Fed. Reg. 5566, 5582 (Jan. 25, 2013)). We find no merit in this argument. The preamble MDA cites discusses the liability of business associates, but the individuals involved in the losses and theft here were all workforce members of the covered entity MDA, not business associates.

There was thus no error in the ALJ's determination that MDA was liable for the three incidents.

III. MDA has shown no error in the ALJ's conclusion that CMPs imposed for the two violations were reasonable.

A. The ALJ did not err in determining the number of violations, or the duration of the period of noncompliance, for the purpose of calculating the CMPs.

MDA argues that CMPs are "remarkable," "incredible" and "excessive," in part because it says OCR and the ALJ erred in finding that, for the purpose of calculating the total CMPs, MDA committed 34,883 violations of the Privacy Rule at section 164.502(a). NA Br. at 3, 4, 28-29, 39. The ALJ properly rejected MDA's arguments about the number of violations it committed, and MDA has identified no error in his analysis.

For MDA's noncompliance with the Privacy Rule forbidding unauthorized disclosure of ePHI at section 164.502(a), OCR proposed, and the ALJ affirmed, a CMP of $1,000 for each of the 31,285 individuals whose ePHI was unlawfully disclosed in the two incidents in 2012 (laptop theft and first thumb drive loss) and for each of the 3,598 individuals whose ePHI was unlawfully disclosed in the incident in 2013 (second thumb drive loss). This resulted in CMPs in excess of the maximum per-year amount "of $1,500,000 for identical violations during a calendar year," but OCR limited the CMP amount for each of the years 2012 and 2013 to the maximum ($3,000,000 total). OCR Br. at 48; 45 C.F.R. § 160.404(b)(2)(ii)(B).

The ALJ upheld OCR's determination that MDA committed 34,883 violations for the purpose of determining the CMP, and rejected MDA's argument "that, at most, it committed three violations of regulatory requirements, asserting that the only violations constitute the theft of a laptop containing unencrypted ePHI and the loss of two unencrypted thumb drives containing ePHI." ALJ Decision at 15. The ALJ concluded that "[i]t is reasonable to count the loss of ePHI for each affected individual as a separate violation" because "[c]ounting the ePHI loss on a per-capita basis reflects the gravity of the loss" and because, "[i]f a violation was limited to the incident in which ePHI was lost (theft or loss of a thumb drive), then a loss of a vast amount of ePHI would count exactly as much as the loss of ePHI pertaining to only one person," a result that the ALJ said "makes no sense." *Id*. at 16.

On appeal, MDA again argues that the CMP should be based on "three alleged violations" and "not 34,883" because MDA "did not 'lose control' of the laptop and two USB drives . . . 34,883 times." NA Br. at 28-29. MDA argues that "[t]he definition of 'violation' in the regulations clearly precludes a focus on the number of patient records contained on any particular device because," in MDA's view, "an alleged 'violation' must focus on the particular 'failure to comply' act." NA Br. at 29 (citing 45 C.F.R. § 160.103).

The plain language of the regulation does not support MDA's view. Section 160.103 states that "[*v*]*iolation or violate* means, as the context may require, failure to comply with an administrative simplification provision." The administrative simplification provision with which MDA failed to comply states that a covered entity "may not use or disclose **protected health information**, except as permitted or required" elsewhere in the regulations. 45 C.F.R. § 164.502(a) (emphasis added). As the essence of MDA's failure to comply with the regulation was its disclosure of **ePHI** of over 34,000 individuals, OCR and the ALJ reasonably concluded that, "in context," each prohibited disclosure of an individual's ePHI was a separate violation under section 160.103. This is consistent with the explanation of "[h]ow violations are counted for purposes of calculating a civil money penalty" in the preamble to the 2013 revisions, which states that–

> Generally speaking, where multiple individuals are affected by an impermissible use or disclosure, such as in the case of a breach of unsecured protected health information, it is anticipated that the number of identical violations of the Privacy Rule standard regarding permissible uses and disclosures **would be counted by the number of individuals affected**.

78 Fed. Reg. at 5584 (emphasis added). That is what the ALJ (and OCR) did here for the noncompliance with section 160.502(a), and doing so was not error. We agree with the ALJ's conclusion that treating the loss of ePHI for a vast number of individuals the same as the loss of ePHI for one individual, which is the essence of MDA's argument, makes no sense because it does not reflect the gravity of the loss.

For MDA's noncompliance with the encryption provision in the Security Rule at section 164.312(a)(2), OCR proposed a per-day CMP of $2,000 for each day of the period of noncompliance, which OCR determined was from March 24, 2011, through January 25, 2013 (674 days), for a total CMP of $1,348,000. OCR Br. at 48. The ALJ agreed, rejecting MDA's claim of only three violations. ALJ Decision at 15-16. He explained: "The violations pertaining to failure to protect ePHI from unauthorized disclosure aren't the specific events resulting in data loss. The daily violations are the ongoing failure by Petitioner to protect patient ePHI from unauthorized disclosure, violations that persisted day after day for years" and "plainly justify imposing per-diem penalties during the period when Respondent was noncompliant." *Id*.

MDA does not address the ALJ's reasoning but merely reiterates its three violations argument. We find no error in the ALJ's conclusion that the duration of this CMP was "reasonable" as "undisputed facts plainly support a finding that Respondent was noncompliant on each day of the period at issue." *Id*. at 15. This approach to determining the penalty is consistent with the regulations.

The preamble language quoted above, which supports counting Privacy Rule violations based on the number of individuals affected, goes on to state that "with respect to continuing violations, such as lack of appropriate safeguards for a period of time, it is anticipated that the number of identical violations of the safeguard standard **would be counted on a per day basis** (i.e., the number of days the entity did not have appropriate safeguards in place to protect the protected health information)." 78 Fed. Reg. at 5584 (emphasis added). The preamble thus supports determining the total CMP for ongoing violations of Security Rule requirements based on the number of days of noncompliance.

Moreover, as the ALJ observed, MDA "was acutely aware of the risks attendant with its failure to protect ePHI," as it "not only identified those risks, but also concluded that there was a high level of risk if it failed to protect such data." ALJ Decision at 15. MDA thus "concluded also that the mechanism that it would use to protect ePHI was to encrypt its mobile devices" but "failed to do so for years." *Id*. The ALJ's explanation of why he found the CMP duration reasonable is supported by the record. As discussed earlier, unchallenged documentation obtained from MDA shows that it identified the high risk to confidential data posed by loss and theft and the need to protect against that risk prior to and during the noncompliance period and that MDA determined to guard against that risk by encrypting portable electronic devices but delayed those efforts in part due to financial considerations. *See supra* at 12-17.

We also note that while OCR ended the period of noncompliance for the purpose of determining the CMP on January 25, 2013, it did not determine that MDA had achieved full compliance with the encryption requirement by that date, but selected that date based on its being the date by which MDA, according to MDA's reporting, had encrypted 98%

of its "managed" computers. Notice of Proposed Determination at 4 n.2 ("OCR determined to end the non-compliance period for this violation on January 25, 2013 in recognition of encryption of [MDA's] managed computer inventory as of that date."); *see also* R. Ex. 51, at 27 (MDA Jan. 25, 2013 letter to OCR). In other words, OCR chose a shorter duration than it could have chosen, to MDA's benefit.

OCR's determination of the period of noncompliance was based on undisputed facts about MDA's recognition of the risk of loss of ePHI, the need to safeguard ePHI, its determination to do so through encryption of its portable electronic devices, and its failure to do so in a manner commensurate with that risk and need. Furthermore, the end date chosen by OCR, an end date short of full compliance, benefited MDA.

We thus find no error in the ALJ's determination that it was "not unreasonable at all to count each day of Respondent's failure to protect its devices as a violation given its assessment of the risk resulting from failure to do so and its inaction in the face of that risk." ALJ Decision at 15.

B. The ALJ did not err in determining MDA's culpability level for the purpose of calculating the CMPs.

The regulations set out four levels or tiers of increasing culpability and impose higher minimum per-violation CMPs for each level. The regulations state that "the Secretary may not impose a civil money penalty—"

> (i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,
> (A) In the amount of less than $100 or more than $50,000 for each violation; or
> (B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
>
> (ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,
> (A) In the amount of less than $1,000 or more than $50,000 for each violation; or
> (B) In excess of $1,500,000 for identical violations during a calendar year
> . . .
> (iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty

> knew, or, by exercising reasonable diligence, would have known that the violation occurred,
>
> (A) In the amount of less than $10,000 or more than $50,000 for each violation; or
>
> (B) In excess of $1,500,000 for identical violations during a calendar year
>
> . . .
>
> (iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,
>
> (A) In the amount of less than $50,000 for each violation; or
>
> (B) In excess of $1,500,000 for identical violations during a calendar year
>
> . . . .

Id. § 160.404(b)(2).

The level OCR chose applies to a violation that "was due to reasonable cause and not to willful neglect," which is the second and second-lowest tier. 45 C.F.R. § 160.404(b)(2)(ii); Notice of Proposed Determination at 5. "Reasonable cause" means "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." *Id*. § 160.401.

The only lower level of culpability provided in the regulations is the first or lowest tier, which applies when the covered entity "did not know and, by exercising reasonable diligence, would not have known" that it violated the requirement at issue." *Id*. § 160.404(b)(2)(i). MDA argues that the facts of this case "compel only a first tier culpability level finding of "did not know." NA Br. at 24.

That level clearly does not apply here. We concluded above that the ALJ did not err in finding that undisputed evidence showed that MDA knew that ePHI was subject to inadvertent disclosure through data loss or theft as early as the 2005 theft of a laptop with information of some 4000 patients. We concluded above that the ALJ did not err in finding that thereafter MDA repeatedly recognized the risk of unauthorized exposure of confidential data resulting from theft or loss of unencrypted portable electronic devices containing such data but that it nonetheless delayed implementing the device encryption that it found a reasonable and appropriate mechanism for protecting such data. ALJ Decision at 6-7, 13-14. Thus, the "did not know" and "would not have known" tier could not have applied.

MDA discounts the ALJ's determinations that MDA was "aware[] of the risk of loss through accidental exposure" but "failed to address the risk that ePHI could be disclosed via theft or loss of mobile devices." NA Br. at 24. MDA argues that the ALJ ignored evidence of MDA's "security mechanisms, available tools, and compensating controls," which, MDA says, demonstrate that it "adequately addressed the risks, and that its employees ignored and acted outside of security protocols designed to address those risks." *Id*. (citing ALJ Decision at 14). As we have already discussed, however, those other measures were inadequate as a matter of law since MDA chose encryption of its portable electronic devices as its reasonable and appropriate mechanism for protecting ePHI but failed to timely implement that mechanism. That failure resulted in disclosure of ePHI via stolen or lost devices that were not encrypted.

For these reasons, MDA is mistaken in relying on an example described in a preamble which assigns the "did not know" culpability level to a hospital whose employee knowingly violates hospital policy by accessing an ex-spouse's paper medical record, does not support its case. *Id*. at 24-25 (citing 75 Fed. Reg. at 40,878-79).[12] That example is not germane in the context of an institution's failure to implement technical safeguards that were required by regulation and that it determined were needed to protect ePHI from accidental disclosure. If anything, the example is notable in that it holds the hospital liable for the employee's actions even though that hospital "had appropriate and reasonable safeguards regarding employee access to medical records[,] had delivered appropriate training to the employee" and "the employee's knowledge of the violation cannot be imputed to the covered entity because the employee was acting adversely to the covered entity." That is, the hospital was still liable for the violation, notwithstanding its lack of responsibility under common law agency principles.

MDA also argues that the first, lowest culpability level applies in the case of the researcher who lost her thumb drive containing ePHI in late November or early December 2013, as it "***occurred after the date*** that the OCR (and ALJ) found [MDA] to be compliant with their hindsight interpretation of 45 C.F.R. § 164.312." NA Br. at 25. However, MDA's noncompliance with section 164.312 was not the basis for the CMP relating to this loss of ePHI in 2013; OCR proposed that CMP for MDA's violation of the prohibition on unauthorized disclosure in the Privacy Rule at section 164.502(a). OCR did not base that portion of the CMPs on any period of noncompliance, but on the fact of the unauthorized disclosure of ePHI for 3,598 individuals. Additionally, as we showed above, OCR did **not** find MDA compliant with the Security Rule encryption provision in section 164.312(a) as of January 25, 2013, but rather chose that date to end the CMP, to MDA's benefit, despite not finding MDA in full compliance.

[12] The preamble is to the Notice of Proposed Rulemaking, *Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act*, proposing the current tiered CMP system and maximum CMP amounts, among other modifications to Parts 160 and 164.

Finally, contrary to MDA's assertion, the ALJ's observation that MDA "could not have known about the specific events that caused ePHI to be disclosed in 2012 and 2013" does not support MDA's argument for the lower level of culpability. *See* NA Br. at 24 (citing ALJ Decision at 14). The observation that MDA could not have known in advance about these specific incidents does not mean that it could not reasonably have foreseen that portable computing devices designed to be carried from place to place, especially thumb or flash drives that are easily removed and can fit in a pocket, could be lost or misplaced, or even stolen. The ALJ recognized as much when, in the next sentence, he dismissed MDA's prior knowledge argument by correctly noting that it "isn't the issue" as MDA "had a clear awareness of the *risk* of loss through accidental disclosure." ALJ Decision at 14. As the ALJ found,

> Allowing unencrypted ePHI to be stored on mobile devices exposed that information to the risk of theft or loss, a risk that Respondent knew about, not only by virtue of the 2005 laptop theft, but because it had repeatedly assessed and discussed that risk. The knowledge of that risk is precisely why Respondent ordered in 2008 that all of its mobile devices be encrypted.

Id. The ALJ thus did not err in determining the MDA's culpability level for the purpose of calculating the CMPs.

C. The ALJ did not err in considering the mitigating and aggravating factors listed in the regulations or in declining to waive the CMPs.

MDA argues that the ALJ erred in declining to reduce the CMPs based on the regulatory mitigating and aggravating factors, as the disclosures caused none of the types of harm listed in the regulation as "[f]actors considered in determining the amount of a [CMP]." 45 C.F.R. § 160.408. These include the "nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to" whether the violation "caused physical harm . . . resulted in financial harm" or "harm to an individual's reputation" or "hindered an individual's ability to obtain health care." *Id*.; *see* NA Br. at 34 ("[T]he facts affirmatively demonstrate a lack of harm resulting from the alleged incident."). MDA argues it "has gone to great lengths to implement meaningful, voluntary corrective actions in response to each incident" and "has ably demonstrated its trustworthiness and dedication to compliance with HIPAA," noting that it "took immediate and voluntary steps to address potential vulnerabilities, and implemented further policies and controls that strengthen its already robust compliance efforts." NA Br. at 35-36 (citing 45 C.F.R. § 160.408(c)(2), (e), calling for consideration of "[w]hether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance" and "[s]uch other matters as justice may require").

We begin by noting that the regulation calls for consideration of the specified factors "which may be mitigating or aggravating **as appropriate**" and does not specify separate mitigating and aggravating factors. 45 C.F.R. § 160.408 (emphasis added). Thus, the ALJ had considerable discretion as to how to weigh these factors. MDA's reiteration of its arguments to the ALJ does not address the ALJ's primary reason for rejecting them: that the proposed per-day CMPs – $2,000 per day for the technical safeguards violation, $1,000 per affected individual for the disclosure violation – are but "a small fraction of the maximum allowable daily amount of $50,000 for second tier [i.e., "reasonable cause"] penalties" and thus "reasonable given that they are so low" and "quite modest given the gravity of Respondent's noncompliance." ALJ Decision at 15, 17. The relatively low per-violation penalties also confirm that OCR already considered the factors in the regulations, as OCR stated in its Notice of Proposed Determination (at 6-7).

The ALJ, moreover, did not increase either of the proposed CMPs as he was authorized to do based on the one aggravating factor he addressed out of several that OCR asserted in the Notice of Proposed Determination, MDA's "failure over a period of years" to implement its choice "to encrypt its devices to address the high risk that it would lose ePHI." *Id*. at 17; *see* Notice of Proposed Determination at 6.[13] MDA argues that any aggravating factors "should be disregarded," but its argument, essentially, is that "the HIPAA Rules have never *required* encryption in the first place" and that "OCR must show a violation of the law, which it did not do," arguments we rejected above as contrary to undisputed evidence and based on an incorrect reading of the regulations. NA Br. at 36. MDA's argument also fails because the ALJ, as noted, affirmed per-violation CMPs near the bottom of the authorized range, indicating he did not accord great weight to any aggravating factors.

We also conclude that the ALJ did not err in finding no basis to waive the CMPs on the ground that they were excessive, as provided in section 160.412 ("Secretary may waive the [CMP], in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation"). ALJ Decision at 17. The ALJ reiterated his points that the CMPs "are reasonable given the gravity of Respondent's noncompliance and the number of individuals potentially affected"; that MDA "knew for more than five years that its patients' ePHI was vulnerable to loss and theft" but "consistently failed to implement the very measures that it had identified as being necessary to protect that information [and its] dilatory conduct is shocking given the high risk to its patients

[13] The Notice of Proposed Determination also referenced MDA's "breach reports to OCR on February 23, 2012, which indicated that, on nineteen occasions in 2011, Blackberry mobile devices containing ePHI were reported as lost or stolen to the University of Texas Police Department." Notice of Proposed Determination at 7. The ALJ did not cite those events, and MDA notes that OCR found no HIPAA violations "and that 'no further OCR action is required.'" NA Br. at 73 (citing R. Ex. 67). Thus, we do not rely on them.

resulting from unauthorized disclosure of ePHI, a risk that Respondent not only recognized but that it restated many times." *Id*. We have already found no error in the ALJ's analyses, his conclusion that MDA violated the two regulations and his conclusion that the per-violation CMPs were reasonable; thus, we need not address those points any further.

MDA, however, focuses on the total CMP amounts, which it contends are excessive and arbitrary and capricious. MDA cites instances in which "OCR closed its case and assessed no penalty" against five health care systems or hospitals and one foundation that were involved in the loss or theft of portable computers (and in one case a cabinet) with unencrypted ePHI of from nearly 40,000 to over a million individuals. "Yet," MDA complains, "only [MDA] is assessed a penalty." NA Br. at 29-32. As the ALJ correctly observed, however, there is "nothing in the regulations that suggests" that the ALJ "evaluate penalties based on a comparative standard," and "doing so would be impractical because a penalty determination in any given case may rest on a myriad of case-specific facts, many of which are not apparent in the documents that announce the imposition of a remedy." ALJ Decision at 16. MDA has alleged no error in this particular observation.

Moreover, MDA has no evidentiary basis to complain that it alone has been penalized. Indeed, its Institutional Compliance Office's September 2012 presentation on the "IronKey Distribution Event," which advised that "[i]t's reasonable and appropriate for [MDA] to encrypt thumb drives," warned of the "potential for fines" resulting from the loss or theft of ePHI. OCR Ex. 49, at 1-2. The presentation noted, for example, that "Alaska Medicaid" had been "fined $1.7 million." *Id*. We have no information about that case and whether it was in any way comparable to MDA's losses of ePHI for over 34,000 individuals, but the reference undercuts MDA's claim that it has somehow been singled out for enforcement.

III. The Board will not reach MDA's argument that the ALJ was not properly appointed under the Appointments Clause.

In *Lucia v. S.E.C.*, 138 S. Ct. 2044 (2018), the Supreme Court held that administrative law judges of the Securities and Exchange Commission are "inferior Officers" of the United States (and not simply federal government employees) who, as provided in the Constitution's Appointments Clause (Art. II, § 2, cl. 2), must be appointed by the President, a court of law, or the head of a department. The Court also held that the "appropriate remedy for an adjudication tainted with an appointments violation is a new hearing before a properly appointed official." 138 S. Ct. at 2055 (internal quotation marks omitted).

Relying on *Lucia*, MDA stated in its Notice of Appeal Brief to the Board that, "[u]pon information and belief, [MDA] contends that the ALJ was not properly appointed under the Appointments Clause of the United States Constitution." NA Br. at 39. As the phrase "[u]pon information and belief" indicates, MDA presented no evidence supporting its assertion; nor did MDA specifically ask the Board to decide the issue or to provide any relief. Instead, MDA stated that it "is raising this issue to the DAB to preserve it for judicial appeal." *Id*. Nonetheless, OCR responded to this assertion in its brief, arguing that MDA had not timely raised the Appointments Clause issue and that the Board had no authority to adjudicate the issue. OCR Resp. at 39-40. Since MDA raised the issue and OCR responded to it, the Board offered MDA an opportunity to reply and OCR an opportunity to respond to any reply. *See Opportunity To Submit A Reply Brief* (Oct. 31, 2018).

After considering the parties' briefs and the regulations governing this appeal, the Board declines to reach the Appointments Clause issue because: 1) the applicable regulations prohibit Board review of this issue since it could have been raised before the ALJ but was not; and 2) the Acting Secretary ratified the appointment of the ALJ, and the Board is not authorized to review decisions of the Secretary.

With certain exceptions not relevant here, "the Board may not consider any issue . . . that could have been raised before the ALJ but was not." 45 C.F.R. § 160.548(e). MDA asserts that it could not have raised the Appointments Clause issue before the ALJ since the Supreme Court did not issue its *Lucia* decision until after the ALJ issued his decision.[14] We do not agree. MDA had reason to know by the end of 2016, approximately seven months before it filed its hearing request, that it could make an Appointments Clause challenge because on December 27, 2016, the Tenth Circuit held in *Bandimere v. S.E.C.*, 844 F.3d 1168, 1188 (10th Cir. 2016) that SEC ALJs were inferior officers. In addition, irrespective of *Bandimere*, MDA could have questioned the constitutionality of the ALJ's appointment at any point during the ALJ proceedings based on the Supreme Court's 1991 decision in *Freytag v. Commissioner of Internal Revenue* (501 U.S. 868), which analysis the Supreme Court in *Lucia* and the Tenth Circuit in *Bandimere* found dispositive. *See* 138 S. Ct. at 2053 (stating that *Freytag* "sa[id] everything necessary to decide this case"); *Bandimere*, 844 F.3d at 1174 (stating that *Freytag* "provides the guidance needed to decide this appeal"). Thus, we conclude that MDA could have raised the Appointments Clause issue at any time during the ALJ proceedings but did not do so, precluding Board review under the regulations governing this appeal.[15]

---

[14] The ALJ issued his decision on June 1, 2018. The Supreme Court issued *Lucia* on June 21, 2018.

[15] Since we do not reach the merits of the Appointments Clause issue, we also do not address MDA's argument that its raising this issue for the first time before this Board (as opposed to at the ALJ level) was timely for purposes of deciding the merits. *See* MDA Reply at 7-8.

Furthermore, while a decision made by the Board under the authority conferred on it by the Secretary's regulations becomes the final decision of the Secretary which can be appealed to federal court, *see* 45 C.F.R. § 160.548(j)(1), (k)(1), the Board has no authority to review a decision made by the Secretary. Acting Secretary Hargan's December 21, 2017, issuance of his "Ratification of Appointments of the Administrative Law Judges" constitutes a decision of the Secretary and, thus, is not subject to review by the Board.

Conclusion

We affirm the ALJ Decision and the penalties the ALJ affirmed.

/s/
Christopher S. Randolph

/s/
Leslie A. Sussan

/s/
Sheila Ann Hegy
Presiding Board Member