AN A.S. PRATT PUBLICATION
JUNE 2021
VOL. 7 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 5** **June 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [143] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

MD Anderson Dodges $4.3 Million HIPAA Penalty After the Fifth Circuit Deems OCR's Actions Arbitrary and Capricious

By Kimberly C. Metzger and Tiffany Kim*

The U.S. Court of Appeals for the Fifth Circuit has vacated a $4.3 million civil money penalty imposed by the U.S. Department of Health and Human Services' Office for Civil Rights against the University of Texas MD Anderson Cancer Center stemming from alleged violations of the HIPAA Privacy Rule and Security Rule. The authors of this article discuss the circuit court's decision.

A three-member panel of the U.S. Court of Appeals for the Fifth Circuit has vacated a $4.3 million civil money penalty ("CMP") imposed by the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") against the University of Texas MD Anderson Cancer Center stemming from alleged violations of the HIPAA Privacy Rule and Security Rule. The Fifth Circuit deemed OCR's enforcement action arbitrary and capricious, in violation of the federal Administrative Procedure Act ("APA").

While regulated entities may greet this decision with a sigh of relief, they should not become complacent: unencrypted portable electronic devices remain one of the fastest routes to breach and rigorous enforcement. Robust employee education, and compliance with internal policies and procedures, is perhaps more important than ever.

WHAT HAPPENED AT MD ANDERSON?

As part of technical safeguards to control access to electronic protected health information ("ePHI"), the Security Rule requires covered entities ("CE") and business associates ("BA") to "[i]mplement a mechanism to encrypt and decrypt electronic protected health information."[1] This is an "addressable" implementation specification; the entity must either implement a mechanism for encryption if it is reasonable and appropriate to do so, and if not, implement an equivalent alternate measure if reasonable and appropriate.[2]

---

* Kimberly C. Metzger is a partner in Ice Miller LLP's litigation group, concentrating her practice in drug and device litigation and data security and privacy, particularly HIPAA privacy compliance. She is a member of the International Association of Privacy Professionals ("IAPP") and is a Certified Information Privacy Professional/U.S. Private Sector ("CIPP/US"), Certified Information Privacy Professional/Europe ("CIPP/E"), and Certified Information Privacy Manager ("CIPM"). Tiffany Kim is an associate in the firm's Litigation and Data Security and Privacy Practice Groups. The authors may be reached at kimberly.metzger@icemiller.com and tiffany.kim@icemiller.com, respectively.

[1] 45 C.F.R § 164.312(a)(2)(iv).

[2] *Id.*; *see also* 45 C.F.R. § 164.306(d) (defining required and addressable implementation specifications).

MD Anderson had determined that encryption was a reasonable and appropriate safeguard to control access to ePHI, and it tried to implement a compliant mechanism for encryption. Specifically, MD Anderson established an "Information Resources Acceptable Use Agreement and User Acknowledgement for Employees" dated January 2009 ("Acceptable Use Agreement"), which stated: "If confidential or protected [MD Anderson] data is stored on portable computing devices, it must be encrypted and backed up to a network server for recovery in the event of a disaster or loss of information." The CE also described encryption requirements in employee newsletters going back to 2010.

In 2012 and 2013, three very bad (and, unfortunately, not uncommon) things happened at MD Anderson, all involving unencrypted ePHI: an unencrypted laptop containing the ePHI of more than 29,000 individuals was stolen from a faculty member's home; a summer intern lost an unencrypted USB thumb drive containing the ePHI of more than 2,000 individuals; and a visiting researcher lost a personal unencrypted USB thumb drive containing the ePHI of more than 3,500 individuals. In all, these incidents affected 34,883 MD Anderson patients.

OCR ENFORCEMENT

MD Anderson self-reported the incidents to OCR. The agency's subsequent investigation revealed several facts that clearly troubled OCR:

- Despite the existence of encryption requirements going back to 2009 (as described in its written policies and employee newsletters), MD Anderson did not begin implementing an enterprise-wide solution to meet those requirements until August 2011, when it launched an encryption project for all desktops and laptops. As of January 25, 2013 (after the first two breaches had occurred), it had encrypted only 98 percent of its managed inventory of 33,385 computers.

- MD Anderson's Information Security Program and Annual Reports for calendar years 2010 and 2011 (before the breaches) identified encryption of confidential data on mobile media as a key risk area "currently not mitigated."

- MD Anderson's Corporate Compliance Risk Analysis for fiscal year 2011 (again, pre-breach) indicated several high-risk findings: (1) no enterprise-wide solution in effect for encryption of laptops and mobile computing devices, and (2) workforce members downloading ePHI and other confidential and restricted information and sensitive data to portable computing devices for use outside the organization.

OCR determined that MD Anderson failed to adequately remediate and manage its "high risk findings" through encryption, as required by the Security Rule and the

entity's own policies, or alternatively, to document why encryption was not feasible and implement an equivalent alternative measure.

After failing to reach informal resolution, OCR issued a Notice of Proposed Determination informing MD Anderson that the agency planned to impose a $4,348,000 CMP. The agency determined that because the devices were never recovered, they were no longer in MD Andersons possession and were unprotected from unauthorized persons. Therefore, MD Anderson had "provided access" to the ePHI stored on them.

This "access" determination is key. The Privacy Rule states that a covered entity such as MD Anderson may not "disclose" PHI except as permitted or required by HIPAA.[3] The HIPAA regulations define "disclosure" to include the "release, transfer, *provision of access to*, or divulging in any other manner of information outside the entity holding the information."[4] OCR determined that by "providing access to" the ePHI on the unencrypted devices, MD Anderson had "disclosed" the information in violation of the Privacy Rule.

OCR enumerated the following HIPAA violations:

- Failure to implement access controls – encryption and decryption, or an equivalent alternative measure – in violation of 45 C.F.R. § 164.312(a)(2)(iv); and
- Impermissible disclosure of the ePHI of at least 34,883 individuals, in violation of 45 C.F.R. § 164.502(a).

After considering MD Anderson's proffered affirmative defenses and waiver arguments, as well as mitigating and aggravating factors, OCR ultimately assessed a penalty of $2,000 per day for the lack of encryption (March 24, 2011 through January 25, 2013) and $1.5 million per year (2012 and 2013) for MD Anderson's unlawful disclosure of ePHI relating to about 33,500 individuals.

MD ANDERSON'S ADMINISTRATIVE APPEALS

MD Anderson appealed through administrative avenues, but the administrative law judge ("ALJ") found in favor of OCR and upheld the penalties against the covered entity.

Notably, the ALJ took a broad view of the technical safeguards a covered entity must implement for ePHI. Rather than focusing on the "encryption and decryption" implementation specification – which is addressable rather than required – the ALJ looked to the higher-level "access control" standard that requires covered entities to

[3] 45 C.F.R. § 164.502(a).

[4] 45 C.F.R. § 160.103 (emphasis added).

"[i]implement technical policies and procedures for electronic information systems that maintain [ePHI] to allow access only to those persons . . . that have been granted access rights. . . ."[5] The ALJ recognized that the Security Rule gives covered entities "considerable flexibility" in determining how they protect ePHI and does not require the use of specific devices or mechanisms. However, the mechanisms a CE or BA adopts – whether encryption or an equivalent alternative measure – "must be effective."

The ALJ affirmed that MD Anderson violated the Security Rule because it did not adopt an effective mechanism for encrypting ePHI. While MD Anderson was not required to choose encryption to implement the Security Rule access control standard (if encryption was not reasonable and appropriate, the CE could have implemented a reasonable and appropriate equivalent), once it did choose encryption, it was "obligated to make it work." And this it "[m]anifestly" failed to do.

The ALJ also considered the alleged Privacy Rule violation: unlawful disclosure of ePHI. MD Anderson pointed to the statutory definition of "disclosure" and argued that the loss or theft of unencrypted devices was not a "disclosure" because OCR failed to show that anyone outside the CE received or viewed the lost ePHI. The ALJ rejected this argument. While disclosure under the HIPAA Rules includes the release of ePHI, the dictionary definition of "release" requires "the act of setting something free," not the recapture of that information by a third party.

Further supporting this interpretation was the fact that OCR's enforcement was not a private claim for damages, which would have required proof of damages resulting from receipt of the lost PHI by someone else.[6]

Finally, the ALJ reasoned that MD Anderson's interpretation of "disclosure" would make this aspect of the HIPAA Rules all but unenforceable: "How could anyone know with any reasonable probability that – for example – the ePHI contained on the stolen laptop resulted in a given individual suffering from identity theft?"

MD Anderson made several other arguments that the ALJ rejected: the lost ePHI was "research information" outside HIPAA's scope, and the actions of the people responsible for the data loss (employees performing "unsanctioned" actions, and a thief) were not imputable to the CE. The ALJ characterized these arguments as a "blizzard" obscuring the real issue: MD Anderson recognized a problem, selected a protective mechanism that included encryption, and failed to effectively implement that mechanism.

[5] 45 C.F.R. § 164.312(a)(1).

[6] In this way, the ALJ distinguished decisions under the federal Privacy Act, which according to MD Anderson held that no cause of action for unauthorized disclosure of confidential information can exist without proof that an unauthorized person actually received the information. The ALJ determined that under HIPAA, the authority to impose a remedy hinges on release of information rather than receipt.

Notably, the ALJ did not consider the constitutional or statutory interpretation arguments raised by MD Anderson due to the limited scope of the ALJ's authority.

Further, when MD Anderson asserted that the penalties were arbitrary and capricious (citing to other instances of ePHI loss that resulted in far more leniency), the ALJ advised that he was not to evaluate penalties based on a comparative standard because the regulations do not prescribe such an approach. Based on the case-specific facts measured against applicable regulatory requirements, the ALJ found OCR's penalties to be reasonable.

APPEAL TO THE FIFTH CIRCUIT

The Fifth Circuit rounded on both OCR and the ALJ and vacated the CMP after determining the penalty violated the APA, a statute that governs how federal administrative agencies propose and establish regulations and grants federal courts jurisdiction over federal agency decisions.[7] Under the APA, a court must "hold unlawful and set aside" agency actions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."[8] Courts will look to whether an agency has examined the relevant data and articulated a satisfactory explanation for its action. Courts reviewing an agency action under the APA will not consider the agency's *post hoc* rationalizations.

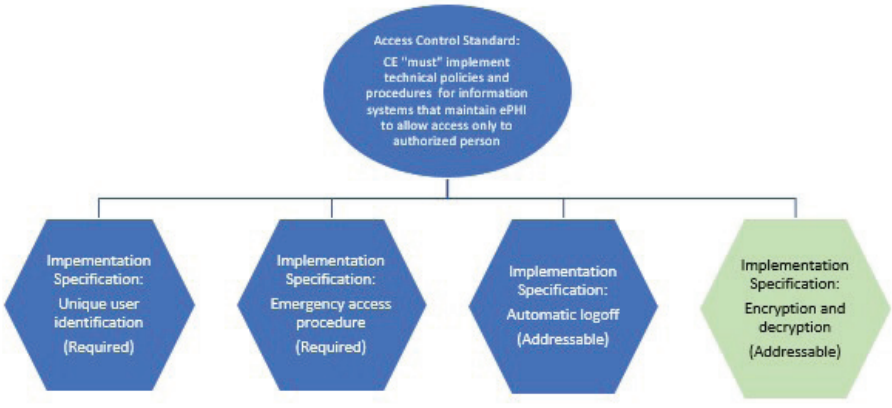
The appellate court determined that HHS's CMP was arbitrary and capricious for four reasons:

1) *MD Anderson implemented "a mechanism" to encrypt ePHI, in compliance with the Security Rule.* The ALJ focused on the overarching Security Rule standard requiring covered entities to implement access controls that limit access authorized persons: the ALJ determined that MD Anderson violated this by implementing an encryption mechanism but not ensuring it was effective. By contrast, the Fifth Circuit targeted the encryption/decryption implementation specification underlying the access standard and determined that MD Anderson had met it simply by implementing "a mechanism" for encryption. It was "undisputed" that MD Anderson had implemented "a mechanism" for encrypting ePHI, namely the Acceptable Use Agreement as well as encrypted thumb drives, a mechanism to encrypt emails, and various mechanisms for file-level encryption in the CE's electronic health record. The real issue, the Fifth Circuit reasoned, was whether the Security Rule required MD Anderson to do more: implement a better mechanism or better implement the chosen mechanism.

[7] Immediately after MD Anderson petitioned for review, HHS "conceded" it could not defend the amount of its penalty and asked the Fifth Circuit to reduce it to $450,000.

[8] 5 U.S.C. § 706(2).

The court determined that MD Anderson was not required to do more in order to comply with the so-called Encryption Rule (the implementation specification supporting the access standard). If encryption was a reasonable and appropriate access control, the Encryption Rule required only that MD Anderson implement "a mechanism" for encryption. It did not require the CE to warrant that its chosen encryption mechanism provided "bulletproof protection" for all systems containing PHI or that all ePHI was "always and everywhere" impervious to unauthorized access.



The court acknowledged that the lost or stolen devices were not encrypted at all. But, the court reasoned, this did not mean MD Anderson failed to implement "a mechanism" for encryption: it just meant the device owners were lax or the MD Anderson was not rigorous enough in enforcing the chosen encryption mechanism. In sum, the court concluded that MD Anderson satisfied the regulation, "even if [HHS] now wishes it had written a different one."

2) *OCR did not prove that MD Anderson violated the Privacy Rule by improperly "disclosing" PHI*. Covered entities may not "disclose" PHI in violation of HIPAA. Seizing on the definition of "disclosure,"[9] the court ruled that disclosure requires "an affirmative act . . . not a passive loss of information." A disclosure also requires that information be "made known" to someone "outside" the covered entity. The court refused to interpret "disclosure" in a way that would allow OCR to prove MD Anderson improperly disclosed PHI without first proving that someone outside the entity received it. OCR could not do that here

[9] "Disclosure" means "the release, transfer, provision of, access to, or divulging in any other manner of information *outside the entity holding the information*." (45 C.F.R. 164.103).

The court acknowledged OCR's argument that this interpretation could make enforcement difficult: "But that's precisely the sort of policy argument that HHS could vet in a rulemaking proceeding."

3) *OCR did not treat like cases alike*. The Fifth Circuit did not like the ALJ's refusal to compare MD Anderson's penalty to others OCR had imposed. In fact, the court called this one of the most remarkable aspects of the ALJ's order. It is a "bedrock principle" of administrative law that an agency must "treat like cases alike" and must supply a reasoned analysis if it changes course. Here, however, MD Anderson proffered examples of other covered entities that violated OCR's interpretation of the Encryption Rule and received no financial penalty. OCR provided no reasoned justification for a multimillion dollar penalty in one case and no penalty in another "like" case.

   OCR argued that it decides cases on their facts, but the court wasn't buying: "an administrative agency cannot hide behind the fact-intensive nature of penalty adjudications to ignore irrational distinctions between cases." Holding otherwise would allow agencies to reward friends and hammer enemies free from scrutiny "because each case is unique." This does not fly under the APA.

4) *OCR based the CMP on "erroneous premises."* After MD Anderson petitioned for Fifth Circuit review, OCR admitted it had misinterpreted statutory penalty caps and conceded it could not defend a fine greater than $450,000. Further, the HIPAA regulations require OCR to consider, in assessing a CMP, whether the alleged violation caused physical, financial, or reputational harm or hindered an individual's ability to obtain health care.[10] While OCR could prove none of those ill effects, the ALJ justified ignoring that premise because the penalties imposed were but a "small fraction" of the maximum amount erroneously presumed to be available under the HIPAA regulations.

In sum, the Fifth Circuit held that HHS acted arbitrarily and capriciously by imposing a significant civil money penalty against a health care provider when:

- The provider – after determining that encryption was a reasonable and appropriate access control – had indisputably implemented "a mechanism" to encrypt PHI, regardless of whether it could have implemented a more rigorous mechanism or enforced the chosen mechanism more rigorously;
- OCR could not prove that unencrypted PHI on the lost or stolen devices had been "made known" to someone "outside" the organization;
- OCR imposed an enormous penalty without engaging in a "like v. like" comparative penalty analysis; and

[10] 45 C.F.R § 169.408(b).

- The penalty amount was based on erroneous premises and grossly disproportionate to the maximum amount OCR later conceded it could defend.

Because OCR offered "no lawful basis" for the imposed penalty, the Fifth Circuit vacated the CMP Order and remanded the matter for further proceedings consistent with the opinion.

KEY TAKEAWAYS

1) *As with all Security Rule requirements, be proactive about encryption.* MD Anderson got out from under a huge penalty, even though the lost and stolen portable devices were not in fact encrypted. While the utter lack of encryption obviously violated the entity's established encryption "mechanism" (i.e., its policies and procedures), the required mechanism was in fact in place. The result almost certainly would have been different at all levels of review if MD Anderson had determined that encryption was a reasonable and appropriate access control but had not implemented a mechanism for encryption. As with all aspects of the Security Rule, if you determine a safeguard is necessary, you must follow through with implementation. Lack of follow-through is often more consequential than ignorance of need.

2) *But do not rest on "implementing a mechanism" for encrypting ePHI.* MD Anderson had determined that encryption was a reasonable and appropriate access control. It was therefore required to "implement a mechanism" for encrypting ePHI. Because there are few situations in which it will be unreasonable or inappropriate for a modern CE or BA to encrypt ePHI, assume that you too must "implement a mechanism" for encryption.

   But is that enough to keep you out of trouble with OCR if the encryption mechanism you implement is ultimately ineffective or unsuccessful? At first glance, the MD Anderson decision seems to say "yes." The court vacated a substantial CMP even though the entity's encryption mechanism was supremely ineffective (the ePHI was not encrypted at all, in direct violation of the encryption mechanism). But remember OCR had enforced against MD Anderson only under the "Encryption Rule" (aka the encryption implementation specification of the Security Rule access standard). However, the Security Rule requires regulated entities to do other things that may implicate the effectiveness of a chosen encryption mechanism, such as:

   - Perform an accurate and thorough risk analysis;[11]

[11] 45 C.F.R. § 164.308(a)(1)(ii)(A).

- Engage in robust risk management;[12]
- Sanction workforce members who fail to comply with Security Rule policies and procedures;[13]
- Implement a security awareness and training program for workforce members;[14]
- Periodically evaluate implementation of Security Rule standards;[15] and
- Secure compliant business associate agreements.[16]

Violate these, and you may find yourself subject to enforcement – even if you have implemented a rock-solid "mechanism" for encrypting ePHI. Notwithstanding the MD Anderson decision, effectiveness does matter.

3) *Consider the effect on breach evaluation and reporting – do you really want to go there?* The Breach Notification Rule defines a "breach" as the "acquisition, access, use, *or disclosure*" of PHI in a manner not permitted by the Privacy Rule, which compromises the security or privacy of the PHI.[17] Given the Fifth Circuit's interpretation of "disclosure" to require that PHI be "made known to" someone outside the organization, it might now be tempting to skip the presumption of breach when there is no way to know whether an unauthorized third party "actually acquired or viewed" unencrypted ePHI on a lost or stolen portable device. Traditionally, actual acquisition or viewing is considered later, as part of a LoProCo (low probability of compromise) analysis to rebut a presumptive breach. The typical order of things:

   - An unencrypted device goes missing;
   - This is considered to be a "disclosure" of ePHI and therefore a presumptive breach per the Breach Notification Rule;
   - A LoProCo analysis is performed to rebut (or not) the presumption; and
   - "Whether the protected health information was actually acquired or viewed" is assessed as a mandatory LoProCo factor.[18]

[12] 45 C.F.R. § 164.308(a)(1)(ii)(B).
[13] 45 C.F.R. § 164.308(a)(1)(ii)(C).
[14] 45 C.F.R. § 164.308(a)(5)(i).
[15] 45 C.F.R. § 164.308(a)(8).
[16] 45 C.F.R. § 164.308(b)(1).
[17] 45 C.F.R. § 164.402 (emphasis added).
[18] 45 C.F.R. § 164.402(2).

Now, however, if there is not a "disclosure" unless PHI is "made known" to someone outside the regulated entity, do you even get to LoProCo without proof that an unauthorized third party actually acquired or viewed the unencrypted PHI? The argument becomes very circular.

The Fifth Circuit opinion notwithstanding, it would be quite risky for a CE or BA facing a lost or stolen unencrypted portable electronic device to unilaterally decide that there is no disclosure (and therefore no presumptive breach) unless and until there is proof that an unauthorized third party actually viewed the ePHI. In most cases, a lost or stolen device stays gone, and there will never be a way to know. The less risky and more privacy-protective path is to presume that unencrypted ePHI on a lost or stolen device has indeed been "disclosed" (if nothing else, under the regulatory definition, "released," "transferred," or "provided") to an unauthorized third party, and therefore that a breach has occurred. Actual acquisition or viewing by (being "made known" to) an unauthorized third party can be considered as it always has: as part of LoProCo to rebut the presumption of breach.

4) *Take care when relying on "like versus like."* The Fifth Circuit made clear that an OCR enforcement may ultimately be vacated as arbitrary and capricious if the agency departs from previous enforcement amounts ("chang[es] its course") without supplying a reasoned analysis. Absent articulated good cause, it must "treat like cases alike." Although the court rather summarily dismissed OCR's argument that it evaluates each case on its individual merits, the fact remains that the HIPAA Enforcement Rule is complex and describes a plethora of aggravating and mitigating factors OCR can consider when determining the amount of a CMP,[19] as well as various affirmative defenses[20] and waiver arguments[21] the CE or BA can assert. Further, each CE and BA comes to the table with a unique structure, function, presentation, set of capabilities, and compliance history. Without an in-depth knowledge of the HIPAA Rules and the facts and circumstances of a particular case, it may be hard (if not impossible) to determine if it is "like" yours and how well another entity's result will translate. Your cases may not be "alike," and even if they are alike – whatever that means – OCR may be able to supply a reasoned analysis of why your case should be treated differently (either better or worse). Hold casual comparisons loosely.

5) *For heaven's sake . . . encrypt portable electronic devices!* OCR has commented time and again in published enforcement: we are long past the learning phase,

[19] 45 C.F.R. § 160.408.
[20] 45 C.F.R. § 160.410.
[21] 45 C.F.R. § 160.412.

> and regulated entities should know and understand the dangers associated with unencrypted portable electronic devices. If you have not assessed these risks, augment your risk assessment and engage in risk appropriate and robust management. Implement entity-specific policies and procedures, inventory your devices, and perhaps most importantly . . . train and educate your workforce. Training involves knowing what to do – education involves knowing why. When workforce members truly understand, appreciate, and internalize the risk associated with a less-than-rigorous approach to encryption, noncompliance will drop, and the documentable effectiveness of your chosen encryption "mechanism" will correspondingly rise.

The Fifth Circuit's decision may encourage covered entities and business associates to exhaust administrative remedies in order to challenge OCR imposed penalties in civil court.