



Voice - (404) 562-7886, (800) 368-1019
TDD - (404) 562-7884, (800) 537-7697
Fax - (404) 562-7881
<http://www.hhs.gov/ocr>

Office for Civil Rights, Southeast Region
Atlanta Federal Center, Suite 16T70
61 Forsyth Street, S.W.
Atlanta, GA 30303

Sent via U.S. Certified Mail and Electronic Mail

July 22, 2019

JUL 22 2019

Judy Ringholz, RN, JD, CHC
VP & Chief Compliance Officer
Office of Compliance and Ethics
Jackson Health System
Jackson Medical Towers
1500 NW 12th Avenue
1st Floor, Suite 102
Miami, FL 33136
Email: judy.ringholz@jhsmiami.org

Re: Jackson Health System
OCR Transaction Numbers: 13-165455, 15-217816, & 16-231802

NOTICE OF PROPOSED DETERMINATION

Dear Ms. Ringholz:

Pursuant to the authority delegated by the Secretary of the United States Department of Health and Human Services (HHS) to the Office for Civil Rights (OCR), I am writing to inform you that OCR is proposing to impose a civil money penalty (CMP) of \$2,154,000 against Jackson Health System (JHS) which is governed by the Public Health Trust (PHT) (created by county ordinance) acting on behalf of the Miami-Dade Board of County Commissioners.

This proposed action is being taken under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), § 262(a), Pub.L. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Section 13410, codified at 42 U.S.C. § 1320d-5, and under 45 C.F.R. Part 160, Subpart D.

I. The Statutory Basis for the Proposed CMP

The Secretary of HHS is authorized to impose CMPs (subject to the limitations set forth at 42

U.S.C. § 1320d-5(b)) against any covered entity, as described at 42 U.S.C. § 1320d-1(a), that violates a provision of Part C (Administrative Simplification) of Title XI of the Social Security Act. *See* HIPAA, § 262(a), as amended, 42 U.S.C. § 1320d-5(a). This authority includes violations of the applicable provisions of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules) and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D), pursuant to Section 264(c) of HIPAA. The Secretary has delegated enforcement responsibility for the HIPAA Rules to the Director of OCR. *See* 65 Fed. Reg. 82,381 (Dec. 28, 2000) and 74 Fed. Reg. 38630 (July 27, 2009). OCR is authorized under the HITECH Act § 13410, 42 U.S.C. § 1320d-5(a)(3), to impose CMPs for violations occurring on or after February 18, 2009, of:

- A minimum of \$100 for each violation where 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, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000.
- A minimum of \$1,000 for each violation due to reasonable cause and not to willful neglect, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed \$100,000. 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.
- A minimum of \$10,000 for each violation due to willful neglect and corrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed \$250,000.
- A minimum of \$50,000 for each violation due to willful neglect and uncorrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed \$1,500,000.
- As required by law, OCR has adjusted the CMP ranges for each penalty tier for inflation. The adjusted amounts are applicable only to CMPs whose violations occurred after November 2, 2015.

OCR is precluded from imposing a CMP unless the action is commenced within six years from the date of the violation.

II. Findings of Fact

1. JHS is a “covered entity” within the definition set forth at 45 C.F.R. § 160.103, and,

as such, is required to comply with the requirements of the HIPAA Privacy, Security and Breach Notification Rules.

2. JHS is a nonprofit academic medical system based in Miami, Florida that operates a number of hospitals and medical centers throughout Florida and provides health care to an average of 650,000 patients annually.
3. JHS creates, maintains, receives, and transmits protected health information (PHI) related to patients who receive health care services from JHS facilities.
4. On August 22, 2013, JHS submitted a Breach Notification Report (“Report”) to OCR. The Report indicated a loss of paper records for 1,471 patients from the Jackson Memorial Hospital’s Health Information Management (HIM) department in January 2013 (“January 2013 loss”).
5. In July 2015, OCR became aware of multiple media reports disclosing the PHI of a JHS hospital patient, a well-known NFL player. An ESPN reporter also shared a photograph of an electronic display board in a JHS operating room and a paper schedule containing the PHI of the same patient.
6. On October 26, 2015, OCR notified JHS that it opened a compliance review relating to the media disclosures of the NFL player’s PHI.
7. On February 25, 2016, JHS timely submitted a Report stating that a photograph was taken of an operating room electronic display board which displayed the PHI of two individuals including “a well-known person in the community.”
8. On February 19, 2016, JHS submitted a Report to OCR reporting that a JHS employee had been selling patient information since July 2011. JHS also reported that 24,188 patients’ records had been inappropriately accessed by the employee since 2011.
9. The Security Rule Security Management Process standard, 45 C.F.R. § 164.308(a)(1), requires that a covered entity must, in accordance with § 164.306, implement policies and procedures to prevent, detect, contain, and correct security violations.
10. In order to implement the Security Management Process standard, a covered entity must comply with the specific requirements or instructions for implementing the standards as set forth in the relevant implementation specifications.
11. Specifically, the implementation specification regarding risk analysis, at 45 C.F.R. §164.308(a)(1)(ii)(A), requires a covered entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic PHI (ePHI) held by the covered entity.
12. In response to several data requests issued by OCR, JHS provided “risk analyses”

conducted on its behalf by third parties in 2014, 2015, 2016 and 2017. JHS also provided internal assessments conducted by JHS in 2009, 2012, and 2013.

13. The risk analyses conducted before 2017 erroneously identified several provisions of the Security Rule as “not applicable” to JHS.
14. The risk analysis completed on September 30, 2014, failed to include all ePHI created, received, maintained or transmitted by JHS (i.e. deficient in scope) and did not identify the totality of threats and vulnerabilities that exist in its systems.
15. Further, the implementation specification regarding risk management, at 45 C.F.R. § 164.308(a)(1)(ii)(B), requires a covered entity to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
16. JHS did not remediate risks, threats and vulnerabilities identified specifically by the 2014 risk analysis to a reasonable and appropriate level. For example, while recommendations were provided by the third party who conducted the risk analysis, JHS did not provide evidence or documentation of a response to those recommendations.
17. A subsequent risk analysis was completed by a third party on September 30, 2015. It did not include all ePHI created, received, maintained or transmitted by JHS (i.e. deficient in scope) and did not identify the totality of threats and vulnerabilities that exist in its systems. Moreover, some sections of the risk analysis were left blank.
18. JHS also did not remediate risks, threats and vulnerabilities identified specifically by the 2015 risk analysis to a reasonable and appropriate level. For example, while recommendations were provided by the third party, JHS did provide evidence or documentation of a response to those recommendations. The same “high risk” threats identified in the 2014 risk analysis were still identified as “high risk” on the 2015 analysis. JHS failed to implement security measures to reduce these risks and vulnerabilities.
19. A subsequent risk analysis was completed by a third party on September 8, 2016. It was not enterprise-wide to include all ePHI created, received, maintained or transmitted by JHS (i.e. deficient in scope) and did not identify the totality of threats and vulnerabilities that exist in its systems. Some sections of the risk analysis were left blank.
20. JHS did not remediate risks, threats and vulnerabilities identified specifically by the 2016 risk analysis to a reasonable and appropriate level. For example, while recommendations were provided by the third party, JHS did not provide evidence or documentation of a response to those recommendations. The same “high risk” threats identified above in the 2014 and 2015 risk analyses were still identified as “high risk” on this analysis. JHS did not provide any evidence that it had made

- efforts to implement security measures to reduce these risks and vulnerabilities.
21. The risk analysis conducted in 2017 was compartmentalized by department and not thorough in scope. For example, only the main campus of JHS was included in the analysis. In addition, the methodology of the 2017 analysis was largely limited to policy review and interviews with staff.
 22. The implementation specification regarding information systems activity review, at 45 C.F.R. § 164.308(1)(ii)(D), requires a covered entity to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
 23. While JHS had the capability to create audit logs and access reports for systems that contain ePHI, it did not regularly review these logs.
 24. Specifically, despite procedures JHS alleges were in place, JHS failed to determine that an employee was impermissibly accessing the ePHI of 24,188 patients for over five years. An anonymous caller notified JHS's Office of Compliance and Ethics on January 4, 2016 that the employee was selling patients' ePHI.
 25. From July 22, 2013 through January 27, 2016, JHS failed to implement policies and procedures to prevent, detect, contain, and correct security violations as required by 45 C.F.R. § 164.308(a)(1). Specifically, JHS failed to conduct an accurate and thorough risk analysis, implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, and implement procedures to regularly review records of information system activity.
 26. The HIPAA Security Rule Information Access Management standard at 45 C.F.R. § 164.308(a)(4) requires a covered entity to implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the HIPAA Privacy Rule at 45 CFR Subpart E.
 27. Among other things, the HIPAA Privacy Rule requires a covered entity to identify persons or classes of persons in its workforce who need access to PHI to carry out their duties, identify the category or categories of PHI to which access is needed, and make reasonable efforts to limit access to the persons and categories identified. *See* 45 C.F.R. § 164.514(d).
 28. JHS admits that for over five years an employee had access to ePHI that she "did not have the proper authorization or authority to access" despite having written policies and procedures in place, demonstrating a failure to implement such policies on an operational basis.
 29. During the course of its investigation, OCR learned that a nurse who treated the NFL player in the operating room and who had legitimate access to his PHI at that time impermissibly continued to access his medical record after she no longer had a job

related reason to do so.

30. Additionally, a second employee was found to be accessing the NFL player's records. This demonstrates users' ability to access ePHI without authorization. While all of these employees were sanctioned, their broad and excessive access evidences a lack of restriction, review and/or modification of the appropriate levels of access to ePHI.
31. From July 22, 2013 through January 29, 2016, JHS failed to implement policies and procedures for granting access to ePHI consistent with the applicable requirements of the Privacy Rule, including restricting access to ePHI to the minimum necessary as required by 45 C.F.R. §164.308(a)(4) and restricting access to the classes of employees who need the ePHI in order to fulfill their job duties as required by 45 C.F.R. § 164.514(d).
32. The HIPAA Breach Notification Rule requires a covered entity to notify the Secretary following the discovery of a breach of unsecured protected health information. 45 C.F.R. § 164.408.
33. Specifically, for breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. 45 C.F.R. § 164.408(b).
34. A breach is treated as discovered by a covered entity as of "the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity" and a covered entity "is deemed to have knowledge of a breach if such breach is known...to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity...." 45 C.F.R § 164.404(a)(2).
35. A JHS employee discovered a loss of paper records in the Health Information Management Department in December 2012 and reported the matter to a JHS supervisor on or before December 31, 2012. These records contained the PHI of 715 patients in three boxes.
36. On January 14, 2013, a JHS employee reported to a JHS supervisor that two boxes of emergency room patient records went missing from the Health Information Management Department. These records contained the PHI of 756 patients.
37. The supervisor did not report the December 2012 loss to JHS Security Services until March 2013, during the JHS internal investigation of the January 2013 incident.
38. In accordance with 45 C.F.R. § 164.408(b), this Report was due to HHS on or before March 15, 2013.
39. JHS did not submit this Report to HHS until August 22, 2013. Thus, JHS was at least

days late reporting 160 days late reporting the breach.

40. Moreover, even though the identified number of individuals affected in this Report included those affected by both the December 2012 loss and the January 2013 loss, the Report only referred to the January 2013 loss.
41. JHS did not submit an addendum to the Report reflecting the December 2012 loss until June 7, 2016.
42. JHS admits that before implementing its HIPAA Privacy Manual & Policies in October 2013 (after the breach involving the loss of paper records), “there were no previous policies as it related to breaches,” including breach response, breach risk assessment, and breach notification procedures.
43. Further, while JHS implemented a breach notification policy in October 2013, the policy does not include specific procedures for effectively providing notification under the Breach Notification Rule.
44. JHS failed to provide timely and accurate notification to the Secretary of HHS of the breach caused by the loss of paper records involving more than 500 individuals. (See 45 C.F.R. § 164.408).
45. On June 17, 2019, OCR issued a Letter of Opportunity and informed JHS that OCR’s investigation indicated that JHS failed to comply with the Security and Breach Notification Rules and that this matter had not been resolved by informal means despite OCR’s attempts to do so. The letter stated that pursuant to 45 C.F.R. § 160.312(a)(3), OCR was informing JHS of the preliminary indications of non-compliance and providing JHS with an opportunity to submit written evidence of mitigating factors under 45 C.F.R. § 160.408 or affirmative defenses under 45 C.F.R. § 160.410 for OCR’s consideration in making a determination of a CMP pursuant to 45 C.F.R. § 160.404. The letter stated that JHS could also submit written evidence to support a waiver of a CMP for the indicated areas of non-compliance. Each act of noncompliance was described in the letter.
46. The Letter of Opportunity was delivered to JHS and received by JHS’s agent on June 17, 2019.
47. JHS submitted its response to OCR’s Letter of Opportunity on July 17, 2019. JHS response stated, “[a]s revealed through our correspondence over the past several years, [JHS] has significantly enhanced its Privacy and Security programs in a number of different ways, and it is committed to continue to improve upon those programs.”
48. JHS’s response did not provide any written evidence of mitigating factors under 45 C.F.R. § 160.408 or affirmative defenses under 45 C.F.R. § 160.410 for OCR’s consideration in making a determination of a CMP pursuant to 45 C.F.R. § 160.404.

49. JHS also did not submit any written evidence to support a waiver of a CMP for the indicated areas of non-compliance.
50. OCR obtained the authorization of the Attorney General of the United States prior to issuing this Notice of Proposed Determination to impose a CMP.

III. Basis for CMP

Based on the above findings of fact, we have determined that JHS is liable for the following violations of the HIPAA Rules and, therefore, is subject to a CMP.

1. JHS failed to implement policies and procedures to prevent, detect, contain, and correct security violations, because it (a) failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by JHS, (b) failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, on a continuing basis through the present, and (c) failed to review system activity in violation of 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), and 164.308(a)(1)(ii)(B) and 164.308(a)(1)(ii)(D). OCR has determined the violation extends the maximum statutory allowed time, which is 6 years, using the earliest date of the violation as July 22, 2013. OCR has determined that the appropriate penalty tier for this violation is reasonable cause.
 - a. Calendar Year 2013: 163 days from July 22, 2013 to December 31, 2013
 - b. Calendar Year 2014: 365 days from January 1, 2014 to December 31, 2014
 - c. Calendar Year 2015: 365 days from January 1, 2015 to December 31, 2015
 - d. Calendar Year 2016: 26 days from January 1, 2016 to January 27, 2016
2. JHS failed to comply with the Information Access Management standard and implementation specification of the HIPAA Security Rule at 45 C.F.R. §164.308(a)(4) when it failed to restrict workforce member access to ePHI to the minimum necessary to accomplish their job duties. OCR has determined that the appropriate penalty tier for this violation is reasonable cause.
 - a. Calendar Year 2013: 163 days from July 22, 2013 to December 31, 2013
 - b. Calendar Year 2014: 365 days from January 1, 2014 to December 31, 2014
 - c. Calendar Year 2015: 365 days from January 1, 2015 to December 31, 2015
 - d. Calendar Year 2016: 28 days from January 1, 2016 to January 29, 2016
3. JHS was in violation of the Notification to the Secretary standard and implementation specification of the HIPAA Breach Notification Rule at 45 C.F.R. § 164.408 when it failed to provide timely and accurate notification to the Secretary of HHS of the breach caused by a loss of paper records. OCR has determined that the appropriate penalty tier for this violation is willful neglect, not corrected.
 - a. Calendar Year 2013: 31 days from July 22, 2013 to August 22, 2013.

IV. No Affirmative Defenses

By its June 17, 2019 Letter of Opportunity, OCR offered JHS the opportunity to provide written evidence of affirmative defenses within thirty (30) days from the date of receipt of that letter. As noted in Paragraph II.47 above, JHS submitted its response to OCR by letter dated July 17, 2019, and did not provide any written evidence of affirmative defenses for consideration under § 160.410. Instead, JHS's response merely referenced the "correspondence" previously provided to OCR "over the past several years." Accordingly, OCR notes that during the course of its investigation, it considered all of the evidence provided by JHS and has determined there are no applicable affirmative defenses.

V. Factors Considered in Determining the Amount of the CMP

In determining the amount of the CMP, OCR has considered the following factors in accordance with 45 C.F.R. § 160.408.

First, OCR considered the nature and extent of the violations. The violations of the Security Rule, identified above, evidence wide-spread and longstanding deficiencies in protecting PHI to prevent impermissible disclosures. For many years prior to OCR's initiation of the above-referenced compliance review, JHS continually failed to conduct a sufficient, enterprise-wide risk analysis that meets the requirements of 45 C.F.R. § 164.308(a)(1)(ii)(A). Further, over the course of many years, no evidence was provided by JHS to support measures implemented to remediate risks, threats and vulnerabilities identified specifically by risk analyses to a reasonable and appropriate level. Additionally, due to JHS's longstanding failure to adequately review information system activity, and failure to limit access to ePHI to the minimum necessary based on job duty, an employee was able to abuse her access to ePHI undetected in JHS systems from 2011 to 2016 and accessed the PHI of 24,189 patients without a job related reason. The employee admitted to selling the PHI of 2,000 of those patients for purposes of identity theft. Lastly, despite JHS's investigation of lost paper records ongoing since January 2013, JHS did not inform HHS of the breach until August 22, 2013 and did not file an addendum to that Report to accurately describe the breach until June 7, 2016. In determining the amount of the CMP, OCR considered the amount of time that JHS remained out of compliance with 45 C.F.R. § 164.308(a)(1), 45 C.F.R. § 164.308(a)(4), and 45 C.F.R. § 164.408 as aggravating factors.

Second, OCR considered the nature and extent of the harm resulting from the violation. JHS identified two employees who in July 2015 accessed the PHI of a NFL player patient without a job related reason to do so. Subsequently, the NFL player's PHI from his treatment at JHS was disclosed by multiple media outlets, including by an ESPN reporter via Twitter. Due to the leak of the NFL player's medical condition, he suffered financial and reputational harm. He suffered an injury to his hand which threatened his reputation as a successful football player. Additionally, the New York Giant's football team rescinded a \$60 million contract offer after the ESPN tweet was posted. Similarly, another JHS employee abused her access to PHI from 2011 to 2016 in JHS systems. She admitted in January 2016 to selling the PHI of 2,000 JHS patients. JHS discovered that she had accessed the PHI of 24,189 individuals without a job related reason.

Third, OCR considered JHS's history of compliance. This action stems from investigations of three different breaches reported in 2013, 2015 and 2016. Further, from 2012-2018, JHS filed approximately 150 "under-500" breach reports. Approximately 391 individuals were affected cumulatively by these "under-500" breaches.

Fourth, OCR considered JHS's financial condition. OCR is cognizant of JHS's position as a public entity that routinely serves low-income and disadvantaged patients. OCR has determined that the CMP amount will not affect JHS's ability to come into compliance or jeopardize its ability to continue to provide health care for patients. JHS is a very large healthcare system with multiple and diverse sources of revenue.

Fifth, OCR has considered JHS's cooperation during this investigation as well as voluntary steps it has taken towards overall compliance. Such mitigating steps include implementing a HIPAA policy manual, restricting physical access to sensitive areas and workstations, implementing automatic logout procedures, appropriately sanctioning workforce members (termination), retraining workforce members regarding identity theft, hiring key compliance personnel (Chief Privacy Officer, Chief Information Security Officer), and purchasing activity review monitoring software.

Lastly, by its Letter of Opportunity, OCR offered JHS the opportunity to provide written evidence of mitigating factors within thirty (30) days from the date of receipt of that letter. As noted in Paragraph II.47 above, JHS submitted its response to OCR by letter dated July 17, 2019, which did not provide any written evidence of mitigating factors for consideration under § 160.408. Instead, JHS's response merely referenced the "correspondence" previously provided to OCR "over the past several years."

Accordingly, as stated in the preceding paragraphs of this section, OCR has considered mitigating factors in determining the amount of the CMP. Therefore, despite the evidence of harm to affected individuals and extended nature of the violations, OCR continues to use the lowest amount in the reasonable cause tier, \$1,000 (\$1,141 after November 2, 2015), for purposes of calculating the penalties for violations under 45 C.F.R. §164.308(a)(1) (security management process), and 45 C.F.R. §164.308(a)(4) (information access management).

VI. Waiver

OCR has determined that there is no basis for waiver of the proposed CMP amount as set forth at 45 C.F.R. § 160.412. JHS presented no evidence that the payment of the CMP would be excessive relative to the violations found here and described in OCR's letter to JHS of June 17, 2019.

VII. Amount of CMP

A. Amount of CMP Per Violation

Based on the above factors, OCR finds that JHS is liable for the following CMPs for each violation described in Section III:

1. Security Management Process – 45 C.F.R. §164.308(a)(1): The CMP is **\$326,000** (see attached chart – Appendix A). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).
2. Information Access Management – 45 C.F.R. §164.308(a)(4): The CMP is **\$328,000** (see attached chart – Appendix A). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).
3. Notice to the Secretary – 45 C.F.R. §164.408: The CMP is **\$1,500,000** (see attached chart – Appendix A). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).

B. Total Amount of CMP

The total amount of CMPs for which OCR finds JHS liable, with regard to the violations described, is **\$2,154,000** (see attached chart – Appendix A).

VIII. Right to a Hearing

JHS has the right to a hearing before an administrative law judge to challenge these proposed CMPs. To request a hearing to challenge these proposed CMPs, you must mail a request, via certified mail with return receipt request, under the procedures set forth at 45 C.F.R. Part 160 within 90 days of your receipt of this letter. Such a request must: (1) clearly and directly admit, deny, or explain each of the findings of fact contained in this notice; and (2) state the circumstances or arguments that you allege constitute the grounds for any defense, and the factual and legal basis for opposing the proposed CMPs. See 45 C.F.R. § 160.504(c). If you wish to request a hearing, you must submit your request to:

Department of Health & Human Services
Departmental Appeals Board, MS 6132
Civil Remedies Division
330 Independence Ave, SW
Cohen Building, Room G-644
Washington, D.C. 20201
Telephone: (202) 565-9462

Copy to:
Serena Mosley-Day, Senior Advisor
Office for Civil Rights
200 Independence Avenue, SW
Suite 523E
Hubert H. Humphrey Building
Washington, D.C. 20201
Telephone: (404) 562-7864

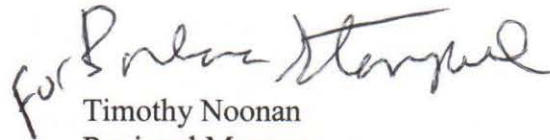
A failure to request a hearing within 90 days permits the imposition of the proposed CMPs without

a right to a hearing under 45 C.F.R. § 160.504 or a right of appeal under 45 C.F.R. § 160.548. If you choose not to contest this proposed CMP, you should submit a written statement accepting its imposition within 90 days of receipt of this notice.

If JHS does not request a hearing within 90 days, then OCR will notify you of the imposition of the CMPs through a separate letter, including instructions on how you may make payment, and the CMPs will become final upon receipt of such notice.

If you have any questions regarding this matter, please contact Serena Mosley-Day, Senior Advisor for Compliance and Enforcement at (404) 562-7864 or at serena.mosley-day@hhs.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "for [unclear] Noonan". The signature is written in a cursive style.

Timothy Noonan
Regional Manager
Office for Civil Rights

Enclosures – Appendix A: CMP Penalty Chart

