KRIEG DEVAULT

Insights

Recent OCR Resolution Agreement and Corrective Action Plan ... Lessons Learned

February 25, 2018

By: Stephanie T. Eckerle and Susan E. Ziel

The Health and Human Services' Office of Civil Rights ("OCR") recently entered into yet another Resolution Agreement after investigating a serious breach incident involving the electronic protected health information ("e-PHI") of over 2 million patients that was maintained by a Florida health care organization.[1] As with so many other past investigations, the OCR made findings that the organization lacked a thorough HIPAA security risk assessment and the necessary security measures and review procedures to safeguard the e-PHI maintained on the organization's information system. Lastly, the OCR determined that the organization had disclosed PHI to third party vendors, acting as business associates, without obtaining satisfactory assurances by way of written business associate agreements.

Under the terms of the Resolution Agreement, the organization was required to pay OCR $2,300,000 to settle the potential civil money penalties associated with the above violations. Additionally, the Resolution Agreement required the organization to enter into a Corrective Action Plan ("CAP") for a two (2) year term that set forth the following terms and conditions:

1. **Compliance Representative.** Designation of an individual Compliance Representative ("CR") responsible for the direction and oversight of the organization's CAP implementation;

2. **Security Risk Analysis/Risk Management Plan.** Completion of a thorough risk analysis and risk management plan and documentation of all security measures implemented to reduce all identified risks and vulnerabilities to a reasonable and appropriate level, all within 120 days of the CAP implementation date;

3. **Policies and Procedures.** Review and revision of certain of the organization's HIPAA policies and procedures with copies submitted to OCR within 90 days, subject to OCR approval;

4. **Distribution of Policies and Procedures to Workforce.** Adoption and distribution of OCR-approved policies and procedures to all existing and newly hired workforce who were subject to the requirements;

5. **Ongoing Review and Update of Policies and Procedures.** Routine review and update of these policies and procedures to reflect any changes in applicable requirements, the organization's operations or other OCR guidance;

6. **Business Associate Accounting/Agreements.** Completion of an accounting of all business associates, in addition to execution of all necessary business associate agreements, with copies submitted to the OCR within 120 days of the CAP implementation date;

7. **Written Plan for Internal Monitoring of CAP Compliance.** Adoption of a written plan to internally monitor the organization's compliance with the CAP, a copy to be submitted to OCR within 60 days of the CAP

implementation date, subject to OCR approval, all of which requires ongoing review and update to reflect any changes in applicable requirements, the organization's operations or other OCR guidance;

8. Assessor. Selection and engagement of a duly qualified "assessor" within 60 days of the CAP implementation date, subject to OCR approval, who is responsible for implementing a written plan that complies with the "assessor's plan" requirements set out in the CAP, again subject to OCR approval, all of which shall result in ongoing assessor "reviews" that are submitted to OCR in regard to the organization's continuing compliance with the CAP;

9. Record Retention. Record retention obligations on the part of the organization, the compliance representative and the assessor;

10. Validation Reviews. Agreement to permit OCR, in its discretion, to conduct any validation review necessary to confirm any assessor review or report; and

11. Mandated Reporting Obligations. Internal reporting obligations that require all workforce with access to the organization's e-PHI databases to report to the compliance representative any violation of the organization's HIPAA related policies and procedures that come to their attention, all of which shall be investigated and reported to both the assessor and OCR to the extent any investigation confirms a violation that qualifies as a reportable event.

Much like the terms and conditions of a Corporate Integrity Agreement, entered into by health care entities and the Health and Human Services' Office of Inspector General ("OIG"), this CAP sets out a very stringent process by which the health care organization is required to implement, monitor and update its HIPAA compliance program under the direction of a designated "compliance representative" and subject to the ongoing review of the OCR and an external "assessor" process. For any HIPAA covered entity or business associate that has endured a reportable breach incident, the prompt implementation of an internal corrective action plan that incorporates many of these interventions may be a very useful (and proactive) risk management tool, even before any OCR investigation or other involvement becomes necessary.

If you have questions regarding HIPAA security risk assessment or other HIPAA-related questions, please contact Susan E. Ziel at sziel@ihsconsultinggroup.com, Stephanie T. Eckerle at seckerle@kdlegal.com, or your regular Krieg DeVault attorney.

[1] https://www.hhs.gov/sites/default/files/21co-ra_cap.pdf.