
19 OCR Right of Access Settlements and Counting: How Covered Entities Should Respond

BLOG | JUNE 2, 2021

Since September 6, 2019, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has announced nineteen settlements under its “HIPAA Right of Access Initiative.” The initiative supports individuals’ right to timely access their health records at a reasonable cost. Despite the COVID-19 pandemic, OCR continues to investigate right of access complaints and pursue corrective action. In 2020, OCR settlements related to the Right of Access Initiative made up over half of the total number of settlements. The settlement agreements reached under this initiative include monetary penalties ranging from \$3,500 to \$200,000, regular OCR monitoring, and detailed corrective action plans. Health care providers should use these settlements as a guide to conduct a risk assessment of their own operations to ensure compliance with a patient’s right of access.

The Right of Access

Under HIPAA at 45 CFR § 164.524, and with certain exceptions, “an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained.” A covered entity is required to provide a copy of the requesting individual’s PHI within thirty days of the receipt of request, in the form and format requested, and for a reasonable fee. When a covered entity or its business associate fails to comply with this right of access, the consequences can be severe. As noted by Acting OCR Director Robinsue Frohboese, “Covered entities must comply with their HIPAA obligation and OCR will take appropriate remedial actions if they do not.” Similarly, according to former OCR Director Roger Severino in 2020, “our Right of Access Initiative is still going strong and [signals] that providers of all sizes need to respect the right of patients to have timely access to their medical records.” OCR “will continue to prioritize HIPAA Right of Access cases for enforcement until providers get the message.”

Using the Corrective Action Plans as a Guide

The corrective action plans (“CAPs”) enforced by OCR under the Right of Access Initiative contain helpful information and insight that can assist covered entities in evaluating their own processes, policies and procedures related to a patient’s right of access. There are several informative aspects of the corrective action plans. Here are four key components that can provide covered entities with practical guidance:

1. Policies and Procedures

The corrective action plans confirm that compliance with HIPAA's right of access provision begins with comprehensive policies and procedures. Each CAP contains a minimum contents section that identifies specific topics to be included in a covered entity's policies. Examples of required content include:

- Procedures to ensure comprehensive and timely responses to access requests;
- Protocols for training all workforce members and business associates;
- Application of appropriate sanctions for workforce members and business associates who fail to comply with the entity's policies and procedures;
- Method for calculating reasonable fees; and
- Process for reviewing business associate performance.

2. Training

Policies and procedures alone, however, are not sufficient. A covered entity's workforce, including business associates, must receive documented training on such policies and procedures. Each CAP requires the covered entity to submit training materials to HHS for review shortly after its updated policies are approved. The covered entity must train its workforce and business associates within sixty days of HHS's approval of the training materials and annually thereafter.

3. Reportable Events & Access Status Reports

Under each CAP, covered entities must promptly investigate allegations of noncompliance with the right of access requirements. If a covered entity determines that a member of its workforce or a business associate failed to comply with the right of access, the covered entity must notify HHS of the failure in writing within thirty days. The written notice must contain several details, including a complete description of the facts, persons involved, the policies impacted, and steps taken by the entity to mitigate harm.

In addition, some entities are required every ninety days under the CAP to submit a list to HHS of each and every access request received by the entity during that timeframe. The list must include the date request received, date request completed, format requested, format provided, number of pages, and cost. If the entity denies any request for access, the entity must submit all documentation supporting the reasons for the denial.

The reporting and status requirements under the CAPs highlight the significant administrative and operational burdens associated with non-compliance under the right of access. Oftentimes, these operational burdens far outweigh the monetary payments that come with the settlements.

4. Business Associates

For providers that employ business associates, the corrective action plans address necessary training, oversight, and monitoring of those business associates. OCR makes clear that providers cannot delegate their responsibility for ensuring a patient's right of access. Regular and documented oversight of business associates is critical to

ensuring compliance with a covered entity's obligations under HIPAA.

If you have any questions or would like to discuss your entity's privacy or security compliance, please contact Young Moore's Health Care Privacy and Security Compliance Team.

The press releases and corrective action plans for each settlement can be found on OCR's News Releases & Bulletins page.

CONTACT US

Phone: 919-782-6860

Fax: 919-782-6753

OFFICE

Young Moore and Henderson, P.A.

3101 Glenwood Ave. Suite 200

Raleigh, N.C. 27612

MAILING ADDRESS

Young Moore and Henderson, P.A.

P.O. Box 31627

Raleigh, N.C. 27622-1627