Blog Post

# Providers: Help is Here to Avoid HIPAA Right of Access Headaches

February 18, 2021
By Kirk S. Davis and Danielle C. Gordet

The Office of Civil Rights (OCR) continues to take seriously all allegations of violations of the HIPAA right of access to patient medical records. As discussed in a previous blog, the OCR is enforcing patient rights by issuing enforcement actions against healthcare providers who fail to provide patients with timely access to their medical records, in accordance with 45 CFR § 164.524(b). It is essential that providers take steps now to avoid future penalties. For purposes of this article the term "provider" refers to a "Covered Entity" under HIPAA, which includes health plans, health care providers (e.g., physicians, hospitals), and health care clearinghouses.

The OCR has settled sixteen enforcement actions (see the chart below of the seven most recent actions and our previous blog, referenced above, summarizing the initial nine). All required that settlement amounts be paid to the OCR and that the parties agree to corrective action plans, which generally are for a term of one to two years.

Upon review of all sixteen corrective actions, we have set forth those provisions OCR has consistently deemed essential to a well-functioning provider organization. The following list contains the most common corrective action plan requirements, though not all sixteen action plans contained every below provision. Nevertheless, implementing as many of these provisions as possible could mitigate potential penalties in the unfortunate event of an allegation of failure to adhere to the right of access standard.

We encourage providers to review this list and ensure that, in the event of an allegation, each item can be "checked off" by OCR.

## Designate a Privacy Official

Providers must designate a Privacy Official who is responsible for the development and implementation of the entity's policies and procedures and responsible for receiving privacy complaints. The Privacy Official should also ensure policies and procedures are developed and implemented, and monitor compliance.

If a practice is small, this does not require a separate hire. A Human Resources or Office Manager can be the designated a Privacy Official. However, it is insufficient to add the title to an existing


### Related People

Kirk S. Davis
Danielle C. Gordet

### Related Work

Healthcare
Healthcare Licensure and Compliance
Hospitals and Health Systems

### Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

employee without also imposing and carrying out the applicable duties.

## Designate an Individual to Review Business Associate Agreement ("BAA") Compliance

Designate one or more individuals, which can include the Privacy Official, who should be responsible for ensuring BAAs with business associates are properly executed. Business associates are people or entities that perform functions that involve the use or disclosure of protected health information ("PHI") on behalf of providers. For example, a business associate may be a third party that assists with claims processing, or a consultant that performs utilization reviews for a provider.

The designated individual should also be responsible for reviewing business associate performance and terminating relationships with business associates who fail to permit the provider to comply with its policies and procedures.

- *Case: An orthopedic practice paid $750,000 to settle allegations that it released patients' x-ray films to an entity that was contracted to transfer the images to electronic media without having executed a BAA. The practice was also required to revise its policies and procedures, including, but not limited to the following: establishment of a process for assessing whether entities are business associates; creation of a standard template BAA; and establishment of a standard process for maintaining BAAs.*
- *Case: A diagnostic imaging company paid $3 Million to settle allegations that it breached the PHI of 300,000 patients. OCR's investigation found that the company did not have BAAs in place with its vendors, including its IT support vendor and a third-party data center provider.*
- *Case: A pediatric practice paid $31,000 after it was discovered that neither the practice nor its business associate, an entity which was contracted to store the practice's records containing PHI, was able to locate a signed BAA.*

## Develop and Implement Required Policies and Procedures

It is necessary to develop and implement written policies and procedures that comply with federal laws governing the privacy of PHI. The policies and procedures should include, but not be limited to, the following:

- **Notice of Privacy Practices**: Providers are required to develop and provide individuals with their Notice of Privacy Practices. The notice should explain how the provider may use and disclose PHI, and the rights that individuals have to their PHI. A policy should be developed which outlines these requirements, including how the notice will be distributed.
    - *Case: A dental practice paid $10,000 to the OCR for failing to have an adequate Notice of Privacy Practices in place.*

- **Right of Access**: There must be a policy regarding an individual's right of access to his/her PHI. Providers are generally required by HIPAA to provide patients or their legal representatives with the ability to inspect or obtain copies of their medical records within 30 days of a request. Procedures must be in place to ensure comprehensive and timely responses to requests for PHI, and a HIPAA compliant process to refuse PHI requests when appropriate. Failure to have these policies and procedures in place may lead to enforcement actions with penalties similar to those outlined in the chart below.
- **Sanctions**: There must be an appropriate sanctions policy and procedure against workforce members who fail to comply with policies and procedures. The procedure should require that the provider document the sanctions, if any, that are applied when there is a violation.
    - *Case*: *A medical practice paid $125,000 to settle allegations that a doctor impermissibly disclosed a patient's PHI to a reporter. OCR's investigation found that the practice failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure.*
    - *Case: A health system paid $2.4 million to settle allegations that it impermissibly disclosed a patient's PHI in a press release. The OCR also discovered that the health system failed to timely document the sanctioning of its workforce members who disclosed the PHI.*
- **Training**: Providers must train their workforce members and relevant business associates regarding HIPAA related policies and procedures. BAAs should include a requirement that business associates participate in trainings and implement the policies and procedures to assure their participation in the trainings and cooperating with the policies and procedures.
    - Each workforce member and business associate who is required to attend the training should certify, in electronic or written form, that he or she has received the training. The training certification should also specify the date training was received.
    - The training materials should be reviewed and updated at least annually, or more often as needed.
    - Larger entities may have the capacity to provide the training to all workforce members and relevant business associates, while smaller entities may not have sufficient resources to devote to this endeavor. A suggestion for smaller entities is to include a contractual obligation in their agreements with business associates that requires the business associates to provide training to their own staff regarding the necessary HIPAA requirements. In addition, providers may want to consider hiring consultants or attorneys who are able to train their workforce members and/or relevant business associates on the relevant policies and procedures.
        - *Case*: *An orthopedic clinic paid $1.5 million to settle allegations of systemic noncompliance with HIPAA,*

*including failure to provide privacy training to workforce members.*

## Update Policies and Procedures

Each year, or more frequently if appropriate due to changed circumstances, providers should assess, update, and revise their policies and procedures. The designated Privacy Official should be responsible for ensuring the necessary updates occur.

## Distribute Policies and Procedures

Providers must distribute updated policies and procedures to all workforce members and relevant business associates, and maintain proof of distribution (e.g., signed or written certifications). All workforce members and relevant business associates should receive all updates in a timely manner.

- *Case: A biotelemetry company paid $2.5 million for "not understanding HIPAA requirements." As part of its findings, the OCR noted that the entity's policies were in draft form and had not been implemented.*

If a provider hasn't implemented these requirements, we urge them to do so right away. Simultaneously, they should institute a continual audit process to ensure that workforce and business associates comply with the provider's policies and procedures on a consistent basis. Auditing assists providers in evaluating whether policies and procedures are being distributed (e.g., if certifications were signed by all required individuals) and adhered to, and whether policies, procedures, and training reflects changes in the law.

OCR enforcement against violations of the right of access is **not** slowing. The OCR has already announced three settlements in the first two months of 2021. In this year's first enforcement action, Roger Severino, the OCR Director, stated: "This first resolution of the year signals that our Right of Access Initiative is still going strong and that providers of all sizes need to respect the right of patients to have timely access to their medical records."

While beyond the scope of this blog, providers must also comply with state law privacy requirements. We strongly urge providers to ensure that the measures discussed in this blog, as well as applicable state requirements, have been appropriately implemented. Failure to do so will likely lead to significant financial penalties. Providers should seek health law counsel to assist in determining how best to proceed.

## Right of Access Enforcement Action

| DATE | ENTITY | LOCATION | PENALTY | APPROXIMATE LENGTH OF DELAY FROM FIRST REQUEST |
|---|---|---|---|---|
| 10/16/20 | Riverside Psychiatric Medical Group | Riverside, CA | $25,000 | 20 months |

| | | | | |
|---|---|---|---|---|
| 10/20/20 | Dr. Rajendra Bhayani (private practitioner) | Regal Park, NY | $15,000 | 26 months |
| 11/12/20 | University of Cincinnati Medical Center, LLC | Cincinnati, OH | $65,000 | 6 months |
| 12/17/20 | Elite Primary Care | Waycross, GA | $36,000 | 13 months |
| 1/6/21 | Banner Health | Pheonix, AX<br>Waycross, GA | $200,000 | 5 month delay with each of the 2 patients' requests |
| 2/2/21 | Renown Health, P.C., | Reno, NV | $75,000 | 11 months |
| 2/3/21 | Sharp HealthCare d/b/a Sharp Rees-Stealy Medical Centers | San Diego, CA | $70,000 | 6 months |

---