

Compliance Today – July 2022 Compliance with new patient right of access rule: Five things to know

By Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB

Rita Bowen (rbowen@mrocorp.com) is Vice President, Privacy, Compliance and HIM Policy at MRO, Norristown, Pennsylvania.

- [linkedin.com/in/rita-bowen-74206012/](https://www.linkedin.com/in/rita-bowen-74206012/)

Disruption is the new normal. As a global civilization dealing with a worldwide pandemic, we've adapted to shifting guidelines, researched dubious news proclamations, and discovered a newfound appreciation for the routine. These three skills converge to support compliance professionals as they monitor HIPAA Right of Access Rule guidelines, research new enforcement actions, and hold steadfast to proven risk mitigation strategies.

This article provides an analysis of the U.S. Department of Health & Human Services' Office for Civil Rights (OCR) enforcement actions, outlines important areas for compliance in 2022, and shares the latest news on states' push to enact their own consumer privacy laws. There are five valuable points for compliance professionals to adopt, research, and discover on their journey toward compliance with the HIPAA Right of Access Rule.

Analysis identifies five failure points

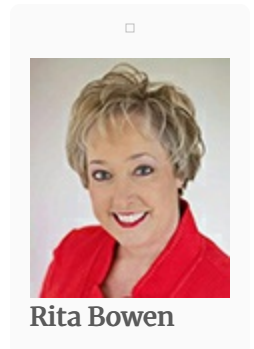
During the 2019 HIPAA Summit, OCR prioritized patient right of access to information as an enforcement priority. Since then, OCR has conducted numerous investigations due to patient complaints about not receiving timely access to their records.^[1] With few exceptions, HIPAA provides patients or their personal representatives the right to access, inspect, and copy their protected health information (PHI).

OCR continues to announce the resolution of investigations to the HIPAA Right of Access Rule on its website. Thus far there have been 27 enforcement actions since the Right of Access Initiative began,^[2] with fines ranging from \$3,500 to \$200,000 and one- to two-year corrective action plans.

To date, the cases fall into five categories of failure. It is important for compliance professionals to understand each of these areas and mitigate properly through awareness, education, and action.

1. Failure to provide information from the defined DRS

The need for a consistent description of the designated record set (DRS) is one of the biggest compliance challenges for 2022. While the Healthcare Information and Management Systems Society, College of Healthcare Information Management Executives, American Health Information Management Association, American Medical Informatics Association, and others continually work to define consistent content for the DRS, the basic definition is a group of records maintained by or for a covered entity that was used in the care of the patient or in the payment of the claim.^[3] This includes items such as medical and billing records, health plan records, and records that are used to make decisions about any individuals.



Rita Bowen

OCR found that one hospital failed to provide fetal heart monitor strips to a patient.^[4] This case involved multiple requests.

The important point for compliance professionals is that any electronic health data used to make healthcare decisions about an individual should be easily accessible to that person.

2. Failure to properly recognize a patient's personal representative

A patient's personal representative has the authority under state law to make healthcare decisions for the individual.^[5] The representative also has the right to access the patient's PHI in a DRS and to direct the covered entity to transmit a copy of the PHI to a designated person or entity of the individual's choice, upon request, consistent with the scope of such representation. Analysis of enforcement actions uncovered cases of adult patients with disabilities who designated a parent to act as the patient representative but the parent was not recognized as such.

3. Failure to respond within the required time frame

Lack of timeliness was cited in several cases when the covered entity failed to respond to the patient request for access according to established timelines, and at a reasonable cost. OCR found that one health system failed to provide a patient with access to the medical record until five months after the initial request.^[6] Records spanning several decades and/or multiple information systems are often the culprit in these cases. Review and update your record retention and destruction policies to mitigate risk of delayed response to patient requests.

4. Failure to recognize the difference between HIPAA authorization and right of access

The PHI that an individual would like to have disclosed to a third party under the HIPAA right of access could be disclosed by a covered entity pursuant to a valid HIPAA authorization. However, there are differences between the two types of disclosure.^[7] The primary difference is that right of access is a required disclosure, and a HIPAA authorization is a permitted disclosure.

5. Failure to update compliance policies, procedures, and documentation

A thorough update of compliance policies is necessary, along with complete documentation of every effort taken to ensure compliance with HIPAA's Right of Access Rule. When OCR enforcement actions occur, thorough documentation may be your most important asset.

While health information management (HIM) professionals are the preferred stewards of patients' requests for records, compliance professionals remain key stakeholders in the effort to mitigate OCR enforcement action risk. To assist, the following section provides further details and explanations related to filling patient right-of-access requests.

This document is only available to members. Please log in or become a member.

[Become a Member Login](#)