Access Denied?
Navigating HIPAA's Right of Access

Stephane P. Fabus, Esq.
Patricia E. Connelly, Esq.

May 19, 2022

Legal Disclaimer

This presentation is solely for educational purposes. The matters presented herein do not constitute legal advice with respect to your particular situation.

Overview

- Understanding the Right of Access
  - HIPAA's requirements
  - Information Blocking implications
- OCR's Right of Access Initiative
  - Enforcement to date
  - Lessons Learned
- Defining the Designated Record Set
- Related Issues
- Practical Takeaways

Right of Access

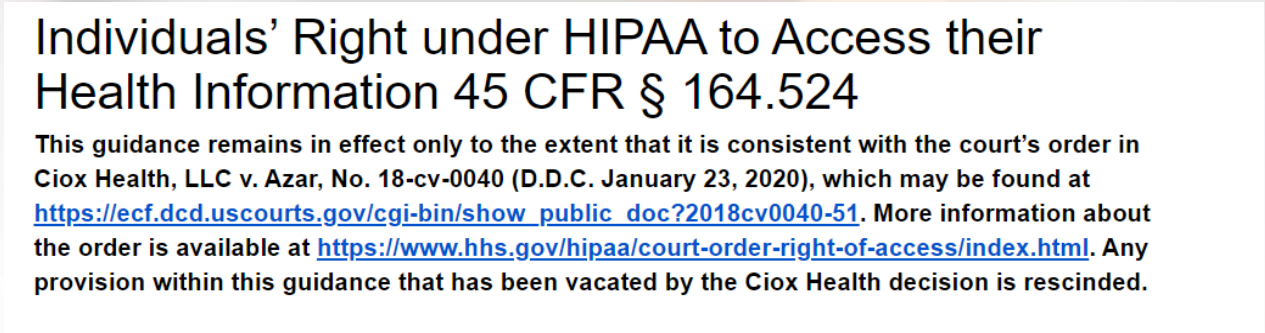
- Individuals may request PHI in multiple ways in multiple ways:
  - Request by individual for information to be provided to the individual (covered by right of access)
  - Request by individual for information to be sent to third party (covered by right of access)
  - Individual authorization permitting third party to request and receive records (**not** covered by right of access) – 45 C.F.R. 164.508
- An individual has the right to access their protected health information contained in the designated record set. 45 CFR 164.524
  - The designated record set includes both paper and electronic information.
  - CE may require the request be in writing (e.g., to assist with identity verification) if notice of requirement is provided
  - CE must provide ability to inspect or a copy of the information in the form and format requested by the individual, if readily producible.
  - Records should be produced within 30 days of the receipt of the request. In limited circumstances the period may be extended by one additional 30-day period.
    - This may be shortened!
  - CE may provide a summary or explanation of PHI in the DRS if agreed to by the individual and any fees imposed are agreed to in advance
  - Regulations limit chargeable amounts to a reasonable, cost-based fee
  - If CE does not maintain the requested PHI, but knows where the requested information is maintained, it must inform the individual where to direct the request for access.
- CE must document the following and retain the documentation:
  - the designated record sets that are subject to access by individuals;
  - The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

How *CIOX* Changed Access Requests

- Ciox Health, LLC v. Azar, et al., No. 18-cv-0040 (D.D.C. January 23, 2020)
- Four holdings:
  1. HITECH Act only requires sending PHI to a designated third party when such PHI is stored in the EHR
     - Such records need only be supplied in an electronic format (not any format requested)
  2. Privacy Rule fee limitations do **not** apply to requests to transmit records to a designated third party
  3. Three (3) methods for calculating proper fees upheld
  4. Exclusion of calculation of labor costs and costs related to retrieval and preparation of information from permissible costs when determining fees upheld

Ciox Health, LLC v. Azar, et al.

- Disclaimer appears on OCR FAQs, but content is unchanged:



Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

This guidance remains in effect only to the extent that it is consistent with the court's order in Ciox Health, LLC v. Azar, No. 18-cv-0040 (D.D.C. January 23, 2020), which may be found at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51. More information about the order is available at https://www.hhs.gov/hipaa/court-order-right-of-access/index.html. Any provision within this guidance that has been vacated by the Ciox Health decision is rescinded.

- Authorized requests by third parties are still not subject to patient rate
  - However, be careful to distinguish third-party directed access requests from authorized requests
- State laws that are "more stringent" continue to apply, so the lowest permitted rate should always be charged
- Ensure business associates processing requests for information are doing so in accordance with changes to the law

Grounds to Deny Access Request

- **Unreviewable Grounds:**
  - PHI is excepted from right of access (i.e.. psychotherapy notes and PHI complied in anticipation of litigation)
  - With respect to an inmate's request, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate
  - With respect to research that includes treatment when the individual has agreed to the denial of access when consenting to participate in the research and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research
  - When PHI is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, if the denial of access under the Privacy Act would meet the requirements of that law
  - When PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information

- **Reviewable Grounds:**
  - When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
  - When the protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
  - if the requestor is a personal representative, when a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

Denying an Access Request

- If the covered entity denies the request, in whole or in part, **it must provide the individual with a written denial,** in accordance with HIPAA's access rules
- Writing must contain:
  - Basis for the denial
  - Right to review
  - How to complain to the Secretary of HHS

A Paradigm Shift

"Give patients electronic modern software control of their medical care, of their chart and of their information."

"The patients have a right to that data."

"Give patients the consumer power that they have in the rest of their lives."

"Give the patient agency"

"I believe an entire ecosystem will build out of that."

"It is the patient's data for the patient to control and move as they desire rather than to be purely in the control of providers and payors."

Don Rucker, M.D.
National Coordinator for Health Information Technology
May 13, 2020, 2020 HIMSS Conference

HALL RENDER | Learn more at hallrender.com.

What is "Information Blocking"?

"Information Blocking" means a practice that:

- Except as required by law or specified by the Secretary pursuant to rulemaking, is **likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information**; and

    - If conducted by a health information technology developer, exchange, or network, such developer, exchange, or network **knows, or should know**, that such practice is likely to interfere with, prevent or materially discourage the access, exchange or use of electronic health information; or

    - If conducted by a health care provider, such provider **knows that such practice is unreasonable** and is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Cures Act - Information Blocking Rule	HIPAA – Privacy Rule
Prohibits an Actor from interfering with access, exchange or use of EHI, unless an exception applies.	Permits Covered Entities to disclose PHI for Treatment, Payment and Healthcare Operations
Actor – means health care provider, health IT developer of certified health IT, health information network or health information exchange.	Covered Entity – Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, associated with the federal healthcare system is a Covered Entity
Electronic Health Information (EHI)* - electronic PHI that would be included in a designated record set without respect to whether such information is in the possession of an entity subject to HIPAA (excluding psychotherapy notes and information compiled for litigation). Excludes psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding	Protected Health Information (PHI) – "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

*From **April 5, 2021 to October 6, 2022**, EHI is limited to information/data elements available in the **USCDI version 1**

.

Information Blocking Exceptions

INFORMATION BLOCKING EXCEPTIONS
Exceptions that involve not fulfilling requests to access, exchange, or use EHI
1) Preventing Harm Exception (45 C.F.R. 171.201) – Reviewable grounds for denial
2) Privacy Exception (45 C.F.R. 171.202) – Unreviewable grounds for denial
3) Security Exception (45 C.F.R. 171.203)
4) Infeasibility Exception (45 C.F.R. 171.204)
5) Health IT Performance (45 C.F.R. 171.205)
Exceptions that involve procedures for fulfilling requests to access, exchange or use EHI
6) Content and Manner Exception (45 C.F.R. 171.301)
7) Fees Exception (45 C.F.R. 171.302)
8) Licensing Exception (45 C.F.R. 171.303)

Current regulations available here. Final rules available here and here. ONC Website and FAQ page available here and here.

Why does it matter?

- Office for Civil Rights (OCR) enforces HIPAA
  - Announced the Right of Access Initiative in 2019
  - This is an ongoing and very active initiative
- Office of the National Coordinator for Health Information Technology (ONC) enforces the Information Blocking Rule
  - No enforcement rule or activity yet, but highly motivated to foster patient access
  - Penalties to include appropriate disincentives for health care providers, up to $1 million per violation for health information networks/exchanges, up to $1 million per violation and potential certification ban for CEHRT for HIT developers
- State Class Action Suits
  - The plaintiff's bar have been pursing class action suits against providers in several states challenging the provision of timely access and the charging of appropriate fees to patients and their representatives

ROA Initiative

- OCR investigating potential violations of an individual's right to access their PHI
  - Right of access includes inspection and copying of PHI in a DRS
- 27 cases since 2019
- Resolution/penalty payments
  - $1,532,650 in fines and penalties
  - $3,500 to $200,000
  - Average appx $60,000
  - often for only ONE patient

HALL RENDER | Learn more at hallrender.com.

From OCR:

"OCR created this initiative to support individuals' right to timely access their health records at a reasonable cost under the HIPAA Privacy Rule."

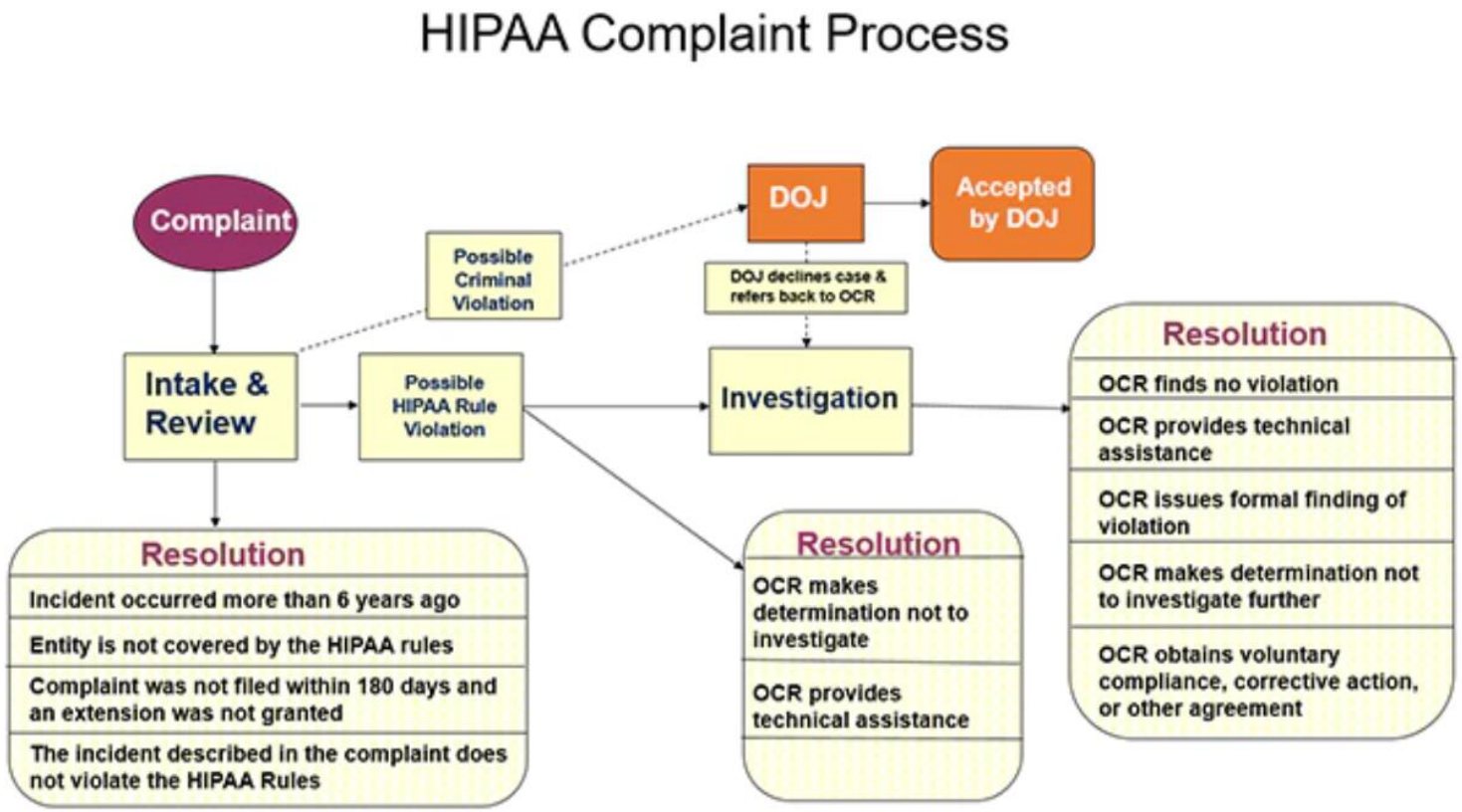
OCR Press Release

March 28, 2022

HALL RENDER | Learn more at hallrender.com.

OCR Enforcement Process

- OCR asking for covered entity financial statements in the first data request
- Technical assistance
- Corrective action plans, monitoring
- Civil Monetary Penalties
- Resolution payments



Enforcement Process, available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

ROA Initiative: Biggest Lessons from Common Themes

- Failing to cooperate with OCR
- Failing to provide a written denial
- Failing to implement technical assistance from OCR
- Lack of timeliness and/or responsiveness
- Improper fees
- Incomplete records

HALL RENDER | Learn more at hallrender.com.

Lack of cooperation with OCR

Case Study

- ***November 2021:*** A physician was assessed a $100,000 penalty for failing to provide copies of records to a patient and for repeatedly failing to respond to OCR investigation letters and communications.

Takeaways

- If you are a HIPAA covered entity, you are subject to OCR's jurisdiction
- Seek legal counsel to push back on requests
- Assess risk and cost of noncompliance/uncooperativeness

Failure to provide a written denial

Case Study

- ***November 2020:*** Hospital did not provide access to PHI because it contained psychotherapy notes. Hospital did not provide a written denial of the request. OCR penalty was $25,000 and provider was instructed to produce all records other than psychotherapy notes.

Takeaways

- Consistently follow Right of Access policies and procedures
- Train staff to recognize when a request is being partially denied
- Do not avoid communicating with patients

Failing to implement technical assistance from OCR

Case Studies

- ***March 2021:*** Hospital paid $65,000 as a result of patient complaint in May 2019 that Hospital had not provided access to PHI. OCR provided technical guidance and the patient complained again in July 2019 that the Hospital still had not provided access to the PHI.
- ***December 2019:*** Clinic paid $85,000 as a result of a patient complaint that the clinic failed to forward the patient's medical records in an electronic format to a third party in a timely manner, and that more than a reasonable cost-based fee was charged. Technical assistance was provided, the clinic did not follow it, and a second complaint was initiated.

Takeaways

- Cannot or will not?
- Seek legal counsel if it is impossible to comply with OCR's technical assistance
- Document how your organization is complying with OCR's technical assistance
- Communicate clearly with the patient to prevent misunderstandings

Timeliness/Responsiveness

Case studies

- ***November 2021:*** Physician practice paid $32,150 for 4-month delay in providing copies of records.
- ***November 2021:*** A treatment center paid $160,000 for a 7-month delay in providing copies of records.

Takeaways

- Treat access requests as a customer service interaction
- Implement policies and procedures and train staff to address:
  - Uncommon requests
  - Clarification of requests
- Understand the role of HIM versus the role of legal
- Be mindful of internal communications and documentation – shared with OCR for proof

Improperly Calculated Fees

Case Studies

- ***November 2021:*** Medical group paid $10,000 related to a complaint that an in-person request was denied, and a flat fee of $25 was charged.
- ***March 2022:*** Psychiatric provider paid $28,000 for not responding to annual access requests for a period of 5+ years, and for requiring the patient to fill out forms in person and imposing a flat fee of $25.

Takeaways

- Determine if offering a free electronic copy is possible
- Justifying fees charged after the fact risks noncompliance
- Document why specific fees are charged
- Regularly review policies and procedures on fees
- State law considerations
  - State law preemption of even HIPAA's flat fees
  - Beware state fee schedule
    - are they your costs or the state's average
- *for example*: special considerations in Wisconsin (Moya)

Failure to provide full set of records

Case Study

- ***September 2019:*** Hospital paid $85,000 to settle a potential violation of ROA for failure to provide a mother with timely access to fetal heart monitor records of unborn child. After nine months, records were provided.

Takeaways

- Important to have a policy that defines the designated record set and that the policy is followed
- Defining DRS is difficult
  - How many systems at your organization contain PHI?
    - EMR, billing system, appointment system, voicemail, e-mail, incident reporting, document management system
    - Are they used to treat the patient?
- Communicating what is and is not available

What is the Designated Record Set?

" Designated record set" is defined as a group of records maintained by or for a covered entity that are:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Any other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

45 CFR 164.501

"Designated Record Set" ≠ "Electronic Health Record"

What does this include? (Examples)

- Provider, nursing and ancillary department documentation regarding health care and services to the patient (consultation, progress notes, orders, assessments, procedure and operative reports, flow sheets, PT/OT, social services, dietary services, etc.)
- History and physical, family medical history, medication records, vitals, etc.
- Data that is linked to the designated record set must also be included, e.g.:
  - X-rays, imaging and radiology reports, images and films
  - Ultrasounds, fetal monitoring strips, heart monitor strips and other tracings
  - Laboratory and pathology tests and results
- Discharge plan and instructions
- Authorizations and consents
- Billing records and claims information
- Case or medical management

HALL RENDER | Learn more at hallrender.com.

What does this not include? (Examples)

- PHI compiled in reasonable anticipation for use in a civil, criminal or administrative action or proceeding
- Incident reports and internal grievance or complaint reports
- PHI in records for financial management or other business and administrative purposes (health care operations)
- PHI in recordings or other materials for quality review or education and training purposes
- PHI in employment records
- PHI held by a business associate that is merely duplicative of PHI in the CE's designated record set, but does not itself actually constitute part of the designated record set
- PHI in information systems that are used for performance improvement, quality control and assessment, utilization management or peer review analyses
- Incomplete test reports. To maintain consistency with CLIA, a test report is complete when all results associated with an ordered test are finalized and ready for release.
  - Similar logic can apply to clinical notes
- PHI from a phone conversation is subject to access only to the extent that it is recorded in the designated record set.
  - Similar logic can apply to other types of communications
- PHI that is not yet part of the designated record set at the time the request is fulfilled

HALL RENDER | Learn more at hallrender.com.

But there continues to be gray areas…

- Provenance – included in USCDIv1, but is a metadata class that may not constitute "health information"
- Communications between patients and providers stored in other systems
- Records received from other providers
- No Surprises Act estimates – must be kept "with the medical record," but is it part of the medical record?
- Research records
- Psychotherapy Notes

HALL RENDER | Learn more at hallrender.com.

Related Issues

- How do we determine what type of request we are dealing with?
- What types of forms should we be using?
- What if we are confused about what the individual is requesting?
- How can we help staff avoid missteps?
- What is we are working with a vendor?

Practical Takeaways

- Review ROI policies and procedures to confirm compliance with all law
  - Are your definitions correct?
  - Do your processes conform with your definitions?
- Consider methods for periodically clearing access request backlogs
- Evaluate and train staff on consistent and standard processing of requests
- Review contracts with vendors to assess compliance and address risk
- Maintain clear and consistent documentation to enable coherent responses to complaints or investigations

Other Privacy News

Keeping an eye on…

- HIPAA regulations
- Part 2 regulations from SAMHSA
- Information Blocking Regulations
  - OIG enforcement?
  - ONC regulations

Presenter Info

Stephane P. Fabus, Esq.
Attorney, Hall Render
sfabus@hallrender.com
(414) 721-0904

Patricia E. Connelly, Esq.
Attorney, Hall Render
pconnelly@hallrender.com
(317) 429-3654

Resources

HIPAA:

- OCR Enforcement Actions here

Information Blocking:

- Current regulations available here
- Final rules available here and here
- ONC Website and FAQ page available here and here

Publications from the Hall Render Team:

- Failure to Timely Provide Records Continues to Pose Significant Risk as Right of Access Initiative Continues
- Failure to Provide Timely Access to Records Results in $85,000 Fine
- Second $85,000 Penalty Issued Under OCR's Right of Access Initiative
- BEWARE: Charging Improper Fees for Patient Access to Records Can Cost Providers Big
- Patients' Access Rights and Permissible Fees Under HIPAA

Information Blocking Toolkit from the Hall Render Team

- Toolkit