

THE INFORMATION BLOCKING RULE: A PRACTICAL GUIDE FOR PRACTITIONERS

June 2022

J. Kevin West
Parsons Behle & Latimer

PARSONS
BEHLE &
LATIMER

parsonsbehle.com

1

MAY 2022 Report of the ONC

- 364 complaints of information blocking (April 2021 to April 2022)
- Sources of complaints:
 - Patients 221
 - Patient reps 53
 - Attorneys 45
 - Healthcare providers 42
 - Health IT developers 26

PARSONS
BEHLE &
LATIMER

2

2

Target of Complaint

- Healthcare providers 291
- Health IT vendors 52
- Other 21

Examples of Complaints

- EHR vendors charging excessive fees to export data to a new EHR software platform
- Delays by healthcare providers in sending records to other providers
- Healthcare providers charging fees for access to ePHI and delays in granting access

Effective Date of Information Blocking Rule

- The 21st Century Cures Act became law on 12/13/2016; Section 3022 of the Act set forth a general prohibition on “information blocking” as to healthcare information and directed HHS to develop rules
- Information blocking rules became effective: April 5, 2021
- Healthcare providers will need to make the same information available on patient third-party applications by October 6, 2022


New Verbiage

Information Blocking



What is Information Blocking?

“A practice that is likely to interfere with, prevent, materially discourage or otherwise inhibit the access, exchange or use of electronic health information (EHI)”

Level of intent required  Actual knowledge (health care providers)
“Knows or should know” (health IT vendors)



Health Care Providers



Health Information Networks (HIN)/Health Information Exchanges (HIE)



Health IT Developer of Certified Health IT

What is Information Blocking?

Information blocking does not include practices that:

1. Are required by law; or
2. Fall within an exception to the information blocking rule

How We Got Here

1996	HIPAA enacted by Congress
2003-2004	HIPAA regs take effect
2009	HITECH Act enacted
2016	21 st Century Cures Act
4/5/21	Information Blocking Rule takes effect

How We Got Here

- HIPAA created a federal right of access for patients
 - Providers had 30 to 60 days to respond to request
 - No right to electronic access
- HITECH Act gave patients the right to obtain access in electronic format
 - Access to be given as soon as possible, but not later than 30 days
 - Limits fees that can be charged to actual, cost-based fees

How We Got Here

- Despite HIPAA and HITECH, patient access still had limitations
 - No real time access
 - EHR systems may limit access due to information blocking features and lack of interoperability

Examples

- Patient had been on beta-blockers, which have a black box warning not to abruptly stop the medication; the EHR system had a warning feature, but the charting portion of the EHR and the medication orders portion did not communicate with each other. A resident stopped the medication, and patient suffered a brain bleed and died

Examples

- A patient had an x-ray of the lung to rule out pneumonia at a hospital. The x-ray showed an infiltrate which was noted on the radiology report. Instead of sharing the report with the treating doc digitally, the radiology department faxed the image, which was severely blurred and difficult to read. The treating doctor did not learn of the findings and patient had severe complications.

How HIPAA and the Information Blocking Rule are Interrelated

- HIPAA does not require real time access; Information Blocking Rule may require it or something close
- As to 3rd parties (everyone but patient), HIPAA usually specifies what may be shared. Information Blocking Rule requires access

Rule of Thumb

Where HIPAA permits disclosure/access of PHI, the Information Blocking Rule will likely require it

“We do not require the disclosure of EHI in any way that would not already be permitted under the HIPAA Privacy Rule. However, if an actor is permitted to provide access under HIPAA, then the information blocking rule would require that the actor provide that access so long as the actor is not prohibited by law by doing so.”

(Official comments to Information Blocking Rule, 4/5/21)

Example

- A PCP asks to see a copy of a treating doctor's records for a mutual patient
 - Under HIPAA the treating doctor is not required to provide the records (though medical ethics may dictate otherwise)
 - Under the Information Blocking Rule, the treating doctor's records must be accessible to the PCP

Example

- A provider's billing service or EHR provider refuses to grant access to records when his/her contract ends with them.
 - HIPAA allowed this to some extent
 - Information Blocking Rule prohibits it

Practices That May Result in Information Blocking

- Contract terms that restrict access to or exchange of electronic health information
- Charging prices or fees that make access cost prohibitive
- Implementing health IT in non-standard ways that increase costs
- Developing health IT in ways that “lock-in” users (i.e., makes it difficult to change vendors/software)

Charging for Access

A. HIPAA:

- 1) Patients may be charged cost-based fees for paper or electronic records
- 2) All others may be charged whatever the health care provider wishes

B. Information Blocking Rule:

- 1) Patients: may not be charged for access to ePHI or to export data to them
- 2) All others: may be charged a reasonable cost-based amount

Healthcare providers now have greater negotiating leverage with respect to –

- Third party billing services
- EHR vendors

The remedy will not be to litigate, but rather to report the matter to the ONC; fines or penalties are paid to ONC, not to the provider

Healthcare provider need to check to see if their EHR software is certified to comply with the Information Blocking Rule

- go to <http://tinyurl.com/y53sqjtt>

In February 2019, the Physician Clinical Registry Coalition reported the following health IT vendors who charged exorbitant fees, imposed technical barriers, etc.

- EPIC
- ALLscripts
- CERNER
- Athena

The New Information Blocking Rule Requires Providers to –

- Make technical changes
- Make operational changes

Technical Changes

Providers must work with IT consultants and EHR vendors to correct technical restrictions on access

Operational Changes

- HIPAA Notice of Privacy practices must be reviewed
- HIPAA Business Associate Agreements may need to be revised
- HIPAA policies will need to be revised
- Staff must get updated training

Information Subject to the Rule

April 5, 2021 – October 5, 2022: data elements in the US Core Data Interoperability (USCDI) standard

- Consultation note
- Discharge summary note
- Procedure note
- Progress note
- Imaging narrative
- Lab report narrative
- Pathology report narrative
- History and physical

After October 5, 2022: ePHI as defined by HIPAA

Enforcement

HIPAA

- Office of Civil Rights (OCR)

Information Blocking

- HHS Office of Inspector General (OIG)

Penalties for Information Blocking Non-Compliance

- Health IT companies –
The OIG may impose civil monetary penalties, up to \$1 million per violation
- Providers – referral by the OIG to an “appropriate agency” for “appropriate disincentives” (still no action on this, but HHS promises to issue proposed rules soon)

HIPAA vs Information Blocking

HIPAA

- 1) Specifies when PHI may be shared w/3rd parties (i.e., other than patient)
- 2) Grants patients the right to inspect and obtain a copy of PHI (paper or electronic) in the designated record set except for psych notes or information compiled in anticipation of litigation

Information Blocking

- 1) Mandates that e-PHI must be accessible to patients and other 3rd parties
- 2) Grants patients/3rd parties access to e-PHI
 - 8 types of records until 10/5/22
 - All e-PHI after 10/5/22

HIPAA vs Information Blocking

HIPAA

- 3) Provider must act on a request for access to PHI within 30 days of the request
- 4) Provider may deny the request for access if:
 - Such would jeopardize the health, safety, security of the patient
 - Record refers to another person & disclosure would create a risk of harm to that person

Information Blocking

- 3) Access to e-PHI must be available at all times
- 4) Provider may deny access if one of “8 exceptions” are satisfied

HIPAA vs Information Blocking

HIPAA

- 5) Access must be allowed in the form (paper or electronic) requested by the patient “if it is readily producible in that form and format”

Information Blocking

- 5) Access must be allowed in electronic format that does not impose unreasonable barriers

HIPAA vs Information Blocking

HIPAA

- 6) Fees –
- a) Patients: providers may charge a reasonable, cost based fee for copies, media, labor and postage
 - b) 3rd parties: providers may charge whatever they wish

Information Blocking

- 6) Fees –
- a) Patients: providers may not charge a fee for allowing electronic access; may still charge for copies, media, etc.
 - b) 3rd parties: providers may only charge a reasonable cost-based fee except for fees to “perform an export of switching health IT or to provide patients their e-PHI”

HIPAA vs Information Blocking

HIPAA

- 7) Defines who may or must have access to PHI

Information Blocking

- 7) Provides that access must be allowed to those who are allowed access under HIPAA

HIPAA vs Information Blocking

HIPAA

- 8) Specifies when a release (authorization) is or is not required in order to share PHI

Information Blocking

- 8) Does not address, but once sharing is allowed, with or without a release, access to ePHI must be allowed

“Our intent is that the information blocking provision would not conflict with the HIPAA Privacy Rule (with respect to the privacy of PHI).”

HIPAA vs Information Blocking

HIPAA

- 9) Patient has the right to request “confidential communications” specifying that PHI may not be shared with certain parties

Information Blocking

- 9) If provider accepts the patient’s request not to share ePHI, this is not information blocking

HIPAA vs Information Blocking

HIPAA

10) HIPAA Security Rule sets a baseline for practices that must be implemented to protect ePHI

Information Blocking

10) Security measures may not unreasonably block access to authorized parties even where such measures are allowed under the HIPAA Security Rule

QUESTIONS ?