ciitizen

The Patient Record Scorecard: Get Into Compliance with the HIPAA Individual Right of Access Before OCR Comes Knocking

Deven McGraw, Chief Regulatory Officer
Former Deputy Director, HHS OCR

1

Ciitizen: Who We Are

Helping cancer patients, using their HIPAA Right of Access, to collect and control all of their health information, so they can use it and share it to meet their needs.

- Get second opinions
- Coordinate with caregivers
- Donate to researchers

2

2

Individuals as “HIEs of One”

The HIPAA Privacy Rule **requires** covered entities to share health information in a ”designated record set” with individuals **upon request** (except in rare circumstances).

Once individuals have their health information, they can **share it with whomever they please.**

How easy is it for individuals to get their health information?

- Harder than it should be
- Access to **complete** records through application programming interfaces (APIs) of certified electronic health records is years away.
- Still a need for greater compliance with HIPAA Right of Access

3

Goals of Presentation

1. Review key components of the HIPAA Right of Individual Access (45 CFR 164.524).

2. Understand common ways that providers fail to comply with the Right of Access, as further described in the following tools evaluating health care provider’s compliance (or likely compliance) with the HIPAA Right of Access:

   Scorecard: patientrecordscorecard.com

   Survey: ciitizen.com/survey

   Whitepaper: https://www.medrxiv.org/content/10.1101/19004291v1

Why We Did the Scorecard and Survey

- OCR released extensive guidance on the Right of Access in 2016* ... but **it didn't appear to have made much of a difference.**
- Recently OCR announced **more robust enforcement** of the Right of Access.
  - OCR settled two cases in 2019 in their new Right of Access enforcement initiative
- We want to **raise the bar on compliance** with the Right of Access – and get processes improved before OCR knocks on the door.
- We're taking a page out of the **quality measurement playbook** – what gets measured and publicly reported gets improved.

* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

5

5

ciitizen

The Patient Record Scorecard

6

The Patient Record Scorecard Process

Request Records
We sent medical record and radiology requests to 210 healthcare providers, based on actual requests from Ciitizen users - patientrecordscorecard.com

Patient Requests Copy
All patients requested digital copies to be populated into their Ciitizen personal health record accounts (options to send through an encrypted portal or by e-mail for text, and CD for images).

Rating
We rated medical providers from 1-5 stars based on their responses.

Scoring
Score is based on the latest request (not averaged) - many scores based on only one request

7

Four Key Right of Access Components

1

Accepts requests by email or fax.

Providers may not create a barrier to access by requiring patients to submit requests in person or by mail

2

Sent in format requested.

The provider sends the records in the format the patient requests, which is in digital form by email for text (option for secure portal), CD for images.

3

Sent within 30 days.

The provider responds to the request within 30 days of receipt (or provides notice of delay and responds within 60 days).

4

No unreasonable fees.

For copies requested by the patient for his/her use, providers may only charge reasonable, cost-based fees for labor of making copy, plus associated supplies

8

Star Rating Key

		STAR RATING - Collapse Requirements		
NON-HIPAA COMPLIANT ★	HIPAA COMPLIANT Substantial Intervention ★★	HIPAA COMPLIANT Minimal Intervention ★★★	HIPAA COMPLIANT Seamless Process ★★★★	HIPAA COMPLIANT Patient Focused ★★★★★
Accepts Requests by Email or Fax	Multiple Supervisor Interventions	One Supervisor Intervention	No Supervisor Intervention	No Supervisor Intervention Accepts External Request Forms Sends Records in 5 Days or Less No Fees

9

9

Access Right – Request Process

- Covered entity **may require written request**; written request required for sending to third party designee.
- Can be **electronic**
- Entity must take reasonable steps to **verify identity.**
- BUT **cannot create barrier** to or unreasonably delay access

For example:
Cannot require individual to make separate trip to office to request access
Cannot require individuals to mail in requests (creates delay)

10

10

Access Right – Request Process *Our Experience*

- Some entities only accept requests by mail; others by fax (far fewer by e-mail).
- Some still requiring patients to come in person (even though guidance makes clear cannot require individual to make separate trip to office to request access.
- Entities struggled with “digital signature” (even with other indicia of identity).

11

11

Form, Format & Manner

- Individual has right to copy **in form and format requested** if “readily producible.”
  - If PHI maintained electronically, **at least one type of electronic format** must be accessible by individual.
  - Depends on **capabilities**, not willingness
  - Scope of this right includes **requested mode** of transmission/transfer of copy
  - **Right to copy by e-mail (or mail),** including unsecure e-mail if requested by individual (plus light warning about security risks)
  - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity’s systems

12

12

Form, Format & Manner *Our Experience*

- Primary reason for noncompliance (scorecard and survey).
- Paper records sent even though request **clearly says electronic** (often with copy of the request at the top of the stack of paper)
- **Refusal** to send by email
- **Refusal** to send by either email or CD unencrypted

Timeliness & Fees

- Access must be provided **within 30 days** (one 30-day extension permitted) BUT expectation that entities can respond much sooner
- **Limited** fees may be charged for copy for patient's own use
  - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable), plus applicable costs for supplies and postage
  - Grabbing info from "portal" (via API) must be free
  - No search and retrieval or other costs, even if authorized by State law
  - Entities strongly encouraged to provide free copies
  - Must inform individual in advance of approximate fee

Timeliness & Fees *Our Experience*

- Often entities **are willing** to provide records for free.
- Others impose fees that seem to have **no link** to HIPAA requirements.
- Continual usage of **state law per page fees**, even for digital copies (plus "basic" or "search and retrieval" fees in some circumstances.)

15

Access Right - Scope *(not rated on Scorecard or Survey)*

- Generally: Designated record set broadly includes all information in the "medical record," as well as other medical, payment, and other records used to make decisions about individuals. Includes images.

Our Experience

- Reliance on printouts from EMR systems (hard to know whether you have all the content)
- Some push back on images, underlying lab data

Right to Direct to Third Parties?

- Prior to 1/27/2020 - Individual's right of access includes **directing a covered entity to transmit PHI directly to another person**, in writing, signed, designating the person and where to send a copy (45 CFR 164.524(c)(3)(ii)).
- OCR opined that fee limitations applied to requests from patients directed to third parties.
- Opinion in CIOX Health LLC v. Alex Azar et al. issued 2/27/2020

17

Right to Direct to Third Parties?

- Opinion in CIOX Health LLC v. Alex Azar et al. issued 1/27/2020
  - Vacated scope of "third party directive" regulation (because it went beyond HITECH)
  - Held that HHS had impermissibly established fee requirements for "third party directives" through guidance
  - Directed HHS to establish fee provisions to implement HITECH third party directive provisions through notice and comment rulemaking.
- HHS statement: "The right of individuals to access their own records and the fee limitations that apply when exercising this right are undisturbed and remain in effect."
  https://www.hhs.gov/hipaa/court-order-right-of-access/index.html

18

Relevant HITECH (2009) statutory language

- HITECH provision (Section 13405(e):
  - In the case that a covered entity maintains an "electronic health record" (broadly defined), the individual has a right to get a copy of such information in an electronic format, and to direct the copy to be transmitted to an entity or person designated by the individual.
  - The fee for providing the individual with a copy of such information "shall not be greater than the entity's labor costs."
  - Electronic health record defined as an electronic record of health-related information on an individual that is created, gathered, managed & consulted by health care clinicians and staff

19

19

19

21st Century Cures (2016) statutory language

- Section 4006(e) – Empowering Patients and Improving Patient Access to their Electronic Health Information (EHI)
  - Secretary, in consultation with ONC, "shall promote policies to ensure a patient's EHI is accessible to the patient *and the patient's designees"* in a manner that facilitates communication w/ the patient's providers and other individuals,including researchers, with the patient's consent.
  - "To promote awareness that an individual has a right of access to inspect, obtain a copy of, and transmit to a third party a copy of the individual's [PHI] pursuant to [HIPAA regulations]," OCR is required to help individuals and providers understand this right, including "best practices for requesting personal health information in a computable format, including using patient portals or third-party apps…."

20

20

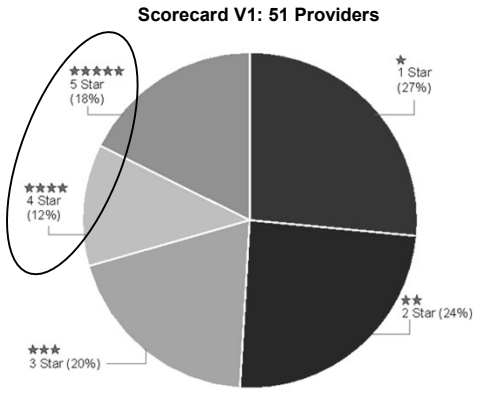
20

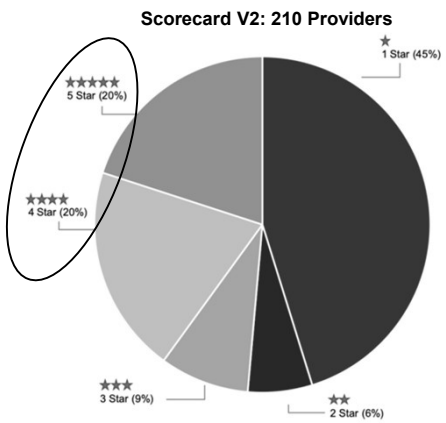
Next Steps

- Clarifying guidance from OCR re: when a patient is requesting his/her own information where an app or service is involved in assisting the patient is needed.
- Ciitizen will continue to do the scorecard but will evaluate how to report information to patients on how providers (and vendors working on their behalf) respond to patient requests using personal health record apps and platforms.

21

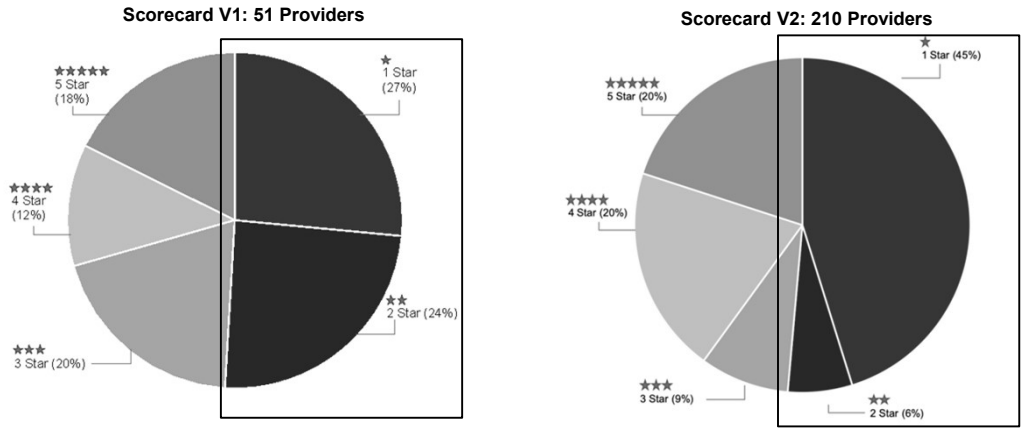
Point 1: good news - more providers delivering seamless access to records.





22

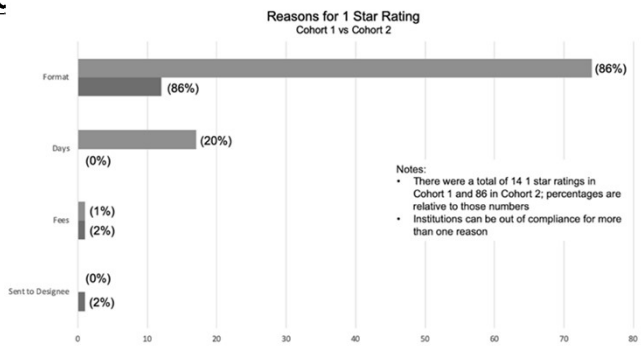
Point 2: bad news - 51% of providers still non-compliant under HIPAA or need significant intervention.



23

23

Point 3: without intervention, too often records aren't released



In this last cohort, we reduced our interventions to providers and saw an immediate increase in number of days it takes providers to send records. Also 20% of non-compliance scores are now associated with providers sending records over 30 days.

24

24

Scorecard 1: Too much intervention needed to get records

	Confirmation Calls per Request	**Medical Records Office Follow-up Calls** per Request	**Escalation Calls** Per Request	**Total Calls** Per Request
Average	2	3	2	7
Maximum	6	8	10	24

Without intervention to HIM Supervisors and/or Privacy Officers, 71% of our requests would not have been fulfilled pursuant to HIPAA requirements.

25

25

Point 4: call and wait times are too long for sick patients!

Hold and Call Times for Select Providers

Provider	Minutes
Provider A	15
Provider B	15
Provider C	15
Provider D	16
Provider E	16
Provider F	16
Provider G	20
Provider H	21
Provider I	22
Provider J	23
Provider K	25
Provider L	25
Provider M	26
Provider N	27
Provider O	34
Provider P	36
Provider Q	36
Provider R	51
Provider S	157

26

26

Point 5: consistency in patient experience an issue

Scores for providers with multiple cases (only most recent reported on Scorecard)

Provider A	3	1			
Provider B	3	4	5		
Provider C	2	5			
Provider D	1	5	1		
Provider E	1	2	4	5	4
Provider F	5	2	5		
Provider G	1	1	1	1	1
Provider H	5	1			
Provider I	3	1	1	1	1
Provider J	1	3			
Provider K	2	1			
Provider L	1	1			
Provider M	2	1			
Provider N	2	1			
Provider O	3	3	3	5	1
Provider P	2	2	2	1	

Majority of providers do not receive the same score for their cases; much variability depending on the HIM representative and potentially other factors.

27

27

citizen

HIPAA Right of Access Survey

28

HIPAA Right of Access Process

Assess
We called healthcare institutions in order to assess *likelihood* of compliance - ciitizen.com/survey

Collect
During the period of August 2018-May 2019 we called and obtained reportable data on ~3,000 institutions

Survey
We asked a set of consistent questions to medical records and radiology departments

Summarize
We summarized our findings in a whitepaper:
https://www.medrxiv.org/content/10.1101/19004291v1

29

Survey questions asked to healthcare providers

Will you accept a patient's access requests by email or by fax?
Some institutions **required the patient to come in** person or to mail a request.

Will you send the records directly to the patient?
Some institutions reported they would **only send the records to another medical professional.**

Will you send the records to a patient by email?
Some institutions **refused to send electronic records by e-mail.**

Do you charge patients for these records – and if so, how much?
Some institutions **shared a fee amount**, more details on next slide.

30

Analysis of Reasonable Fees

Per <u>OCR guidance on the Right of Access:</u>

- We considered an institution to **be charging "reasonable fees"** if they:
  - did not charge patients
  - Charged a flat fee of $6.50 or less, or reported fees that seemed to be based on reasonable labor costs for copying
- We considered an institution to **be charging "unreasonable fees"** if they:
  - Charged per page fees, including fees for records retrieval, or charged a flat fee higher than $6.50
- Institutions who did not answer this question are reported as **NA** (not applicable)
- When answers **suggested** compliance, we gave institutions credit.

31

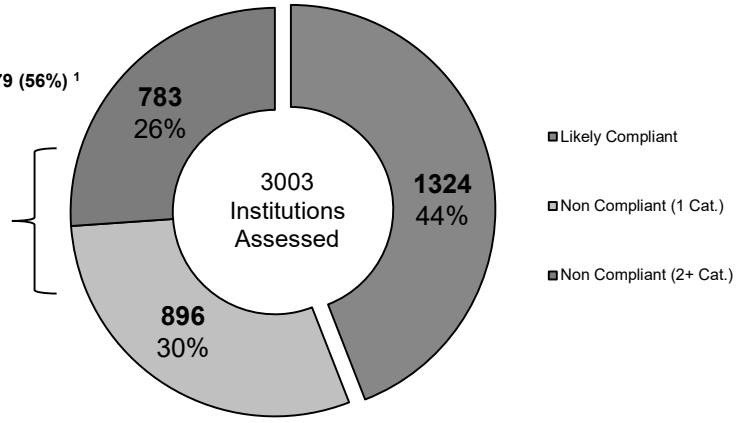
31

HIPAA Right of Access Survey Analysis

Likely Non-Compliant Institutions = 1,679 (56%) [1]

Primary Reasons for Non-Compliance[2]

1. Refusal to send records to patients electronically (either by email or by upload into a secure portal for text records, or by mailed CD for images), n=1423
2. Non-compliance with fees[3], n=727
3. Refusal to send records/images directly to patient, n=344



Notes

1. Non-compliance in at least one category indicates overall non-compliance. This is because all components are legally required to be compliant
2. Institutions can be non-compliant for more than one reason
3. **We also found that of the 727 institutions non-compliant with fees, 521 (72%) were also non-compliant in another category**

32

32

Our scorecard and survey show similar results

	Scorecard	Survey
Overall non-compliance/compliance only with multiple interventions	51%	56%
% of non-compliant (or likely non-compliant) providers refusing to send records electronically by email	85%	85%

33

33

Potential Limitations of Scorecard & Survey

- Many providers were scored based on one request
  - For HIPAA compliance with the right of access, being compliant with each request matters
  - But makes meaningful statistical analysis more difficult
- We took detailed notes but did not record interactions (neither for scorecard nor survey)
- Phone surveyors worked from scripts but we lacked reporting conventions for fee information
- Providers evaluated separately by location

34

34

Healthcare provider compliance with HIPAA critical to patients over next few years.

- **Still too much non-compliance out there** – too hard for patients to exercise their right of access, particularly when they both don't know enough about HIPAA to push back or have the time and energy to fight these battles
- Direct access by patients to their records in Electronic Health Records (EHRs), particularly through open, standard APIs, **will become more robust** – but it will take years before this is fully implemented, especially for the entire "designated record set"
- We will still need medical records offices – **and their vendors** – to be compliant with the Right of Access for some time to come

35

35

New Rules – EHR Certification & Information Blocking

- Pre-publication final rules released in early March 2020. Still need to be official published in Federal Register. (https://www.healthit.gov/sites/default/files/cures/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf)
  - Certified EHRs must make U.S. Core Data Set for Interoperability available to patient-facing apps (via APIs) w/in two years of publication.
  - Certified EHRS must have capability to export all of a patient's ePHI w/in three years of publication.
  - Information blocking rules prohibit charging of impermissible fees, processes that make obtaining information more difficult that they should be – esp. for patients.
  - Health plans overseen by CMS must make claims data available via APIs by January 1, 2021. https://www.cms.gov/files/document/cms-9115-f.pdf

36

36

What's next?

1

We will continue to do **rolling updates to the scorecard** - updating the scores of existing providers and adding new providers

2

We are exploring how to **update the survey**

3

Continue **free webinars** to educate providers on the right of access; private webinars and assessments also possible.

37

37

38