Deven McGraw, JD, MPH, LLM
General Counsel & Chief Regulatory Officer
Ciitizen

Patient Control of Health Data

- Chief Regulatory Officer & General Counsel, Ciitizen (November 2017-present)
- Deputy Director, Health Information Privacy, HHS Office for Civil Rights (June 2015-October 2017)
- Acting Chief Privacy Officer, HHS Office of the National Coordinator for Health IT (January 2017-October 2017)
- Partner, Manatt Phelps & Phillips, LLP (March 2014-June 2015)
- Director, Health Privacy Project, Center for Democracy & Technology (March 2008-March 2014)
- Chair, Privacy and Security “Tiger Team,” Health IT Policy Committee (established in HITECH) (2009-2015)

Individuals as the “wormhole” for data portability

- HIPAA’s permissive sharing provisions are “may share” (not must). In contrast, entities MUST share 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 APIs is years away.
  - Still a need for greater compliance with HIPAA access right.

HIPAA Right of Access

- 45 CFR 164.524
- Comprehensive guidance (fact sheet & FAQs) issued in early 2016 - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- Covers the following:
  - Scope
  - Form and Format and Manner of Access
  - Timeliness
  - Fees
  - Directing Copy to a Third Party, and Certain Other Topics

Access Right - Scope

- Generally: Designated record set broadly includes medical, payment, and other records used to make decisions about individuals.

- Our experience:
  - Reliance on printouts from EMR systems
  - Push back on images

Access Right – Request Process

- Covered entity may require written request – written request required for sending to third party designee
- Can be electronic
- Reasonable steps to verify identity
- BUT cannot create barrier to or unreasonably delay access
  - E.g., cannot require individual to make separate trip to office to request access

Access Right – Request Process

- Our experience:
  - Some entities only accept requests by mail; others by fax (far fewer by e-mail)
  - Entities struggle with “digital signature” (even with other indicia of identity)
  - Need set of best practices for identity
  - Some still requiring patients to come in person

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
  - –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

Form, Format & Manner

- Our experience:
  - Still getting records sent on paper (clearly paper copies of EMR data) (+invoice)
  - Refusal to send by unsecure e-mail, notwithstanding patient request & acknowledgement of security risks
  - Images come by CD (too large for e-mail)

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
  - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if 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
  - Still use of state law fees (plus “basic fees” in some circumstances)

Right to Direct to Third Parties

- 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)
- Same provisions re: timing, fees, form & format (etc.) apply

Right to Direct to Third Parties

- Our experience:
  - Some data sent to patients instead of third party designee
  - Record release offices/staff still not accustomed to this aspect of the Rule.

Next steps

- In the future, more and more PHI will be available through APIs
  - ONC & CMS proposed rule – comments due May 4
  - Impact of proposed information blocking rules unclear
  - To leverage their access rights, patients will still need functioning medical records offices/staff for some period to come
  - Increased OCR enforcement per recent announcement

ciitizen | we can do more. together.

Deven McGraw, Chief Regulatory Officer & General Counsel
deven@ciitizen.com
www.ciitizen.com
@healthprivacy