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

SDOH & Data Sharing - Complying with HIPAA & Delivering whole Person Care

- 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)

Privacy Protections Matter

- Help assure people will seek care for sensitive health conditions
- 1/8 withhold information or decline to seek treatment due to concerns about confidentiality
- Of particular concern for sensitive health information - for example, as many as 1/4 adults in a given year is suffering from a diagnosable mental disorder, and nearly 2/3 do not seek treatment due in part to fear of disclosure, potential rejection from friends, and discrimination

SDOH Data can be sensitive

- Social determinants data may be collected directly from patient (such as through conversation) or collected without the patient's knowledge
- Latter type in particular = not type of data patients expect clinical professionals to have

U.S. Protections for Health Data

- HIPAA
  - Applies only to “covered entities” and their “business associates”
  - Covers identifiable information (known as protected health information or PHI)
  - Specific provisions re: how data can be “de-identified” (very low (NOT zero) risk of re-identification)
  - Does not preempt stronger state laws
- Also federal laws protecting identifiable information from a federally-supported substance abuse treatment program (Part 2) and protecting health info held by an educational institution (FERPA)
- FTC authority to crack down on “unfair” and “deceptive” trade practices

HIPAA

- Covered entities: most health care providers, all health plans, health care clearinghouses
  - All defined in the regulations (45 Code of Federal Regulations (CFR) Part 164)
- Business associate: an entity that "creates, receives, maintains or transmits" PHI in fulfilling certain functions or activities on behalf of a covered entity. (45 CFR 160.103).
- Examples of BAs:
  - EMR vendors (Epic, Cerner, etc.)
  - HIEs (CareSpark, SHINY, etc.)
- Not a BA: FitBit; pharma companies (for example)

If covered by HIPAA, what data is covered?

- HIPAA treats all health information the same (except psychotherapy notes, when they are kept separate from other data)
- Definition of PHI is broad: "relates to the past, present, or future physical or mental health or condition of an individual; *the provision of health care to an individual*"; or payment for care (emphasis added).
  - Health care "means care, services or supplies *related to* the health of an individual."
  - It includes, "but is not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling service, assessment or procedure [with regard to] the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body."

HIPAA's "limits" on collection

- Not many
- "Minimum necessary" standards *may* apply (164.514(d)(4))
- A covered entity must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, *when requesting such information from other covered entities*.
- (if not requesting from other covered entities) Must develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made; and
  - Must review requests for *disclosure* on an basis in accordance with such criteria.
- But the minimum necessary standard does not apply to requests for treatment!

Once the data is in the door…HIPAA's Rules (very high level summary!)

- Fairly detailed regulatory provisions
- Privacy Rule - medium agnostic
  - Establishes permitted uses and disclosures - for example, TPO
  - Requires express individual authorization for other uses/disclosures
  - Individual rights provisions
- Security Rule - digital data only
  - Requires security risk assessment and plan to address/mitigate identified risks
  - Technical, administrative & physical safeguards - required/addressable implementation specs
- Breach Notification Rule - medium agnostic; safe harbor for data encrypted to NIST standards

Resources on HIPAA & SDOH

- **Privacy Concerns Related to Inclusion of Social and Behavioral Determinants of Health in Electronic Health Records** https://www.ncbi.nlm.nih.gov/books/NBK269329/
- Data Driven Justice and HIPAA – Frequently Asked Questions http://www.naco.org/sites/default/files/documents/DDJ%20HIPPA%20FAQs.pdf

HIPAA Individual Rights

- Right of individual to access (and receive copies of) health information
- Right of individual to request amendments to health information
- Right of individual to request restrictions (not required to be honored except when individual pays in full)
- Note: all individual rights can be exercised by personal representatives (but these are persons who, by law, are authorized to make health care decisions for the individual)
  - Exception in circumstances where provider suspects abuse

Individuals as the “wormhole” for data portability

- HIPAA’s permissive sharing provisions are “may share” (not must) In contract, entities MUST share with individuals upon request (except in rare circumstances)
- Individuals then have the right to digital copies of their health information (all of it – including SDOH collected in the record), which they can then share with whomever they please

HIPAA Right of Access

- Issued in two phases in early 2016 - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- Comprehensive Fact Sheet & series of FAQs
  - Scope
  - Form and Format and Manner of Access
  - Timeliness
  - Fees
  - Directing Copy to a Third Party, and Certain Other Topics

Access Right - Scope

- Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  - Doesn't matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports , progress notes and underlying information (including genomic information)
  - Does not include psychotherapy notes if they are kept separate from the other information in the EMR
  - Includes SDOH data collected about an individual (because used to make decisions about individuals)

Access Right - Scope

- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access

Access Right - Reqs

- Covered entity may require written request
- 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

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

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 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

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

Sharing information w/caregivers

- Individual can use right of access to have information sent to caregivers (part of right of access so must share unless exception applies)
  - If caregiver is personal representative, they stand in the shoes of the individual w/r/t exercising right of access
- Providers also permitted to share information relevant to the care of the individual (or payment)
  - Only information relevant to care/payment (may/may not include SDOH)
  - Sharing permitted, not required
  - Great new resources:
    - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_ffg.pdf
    - https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf

ciitizen | we can do more. together.

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