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

Data and/or Your Life: The Balance Between Interoperability and Privacy

- 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
- 1/6 (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

Building Trust in Appropriate Data Uses

- Aim of protections is to enable appropriate use
- Fair information practice principles (FIPPs) built on concept of responsible data stewardship
  - Model for privacy laws in US and internationally
- Privacy by Design (Ann Cavoukian)

HHS ONC FIPPs (2008) (one model)

- Individual Access
- Correction
- Openness & Transparency
- Individual Choice
- Collection, Use and Disclosure Limitation
- Data Integrity & Quality
- Safeguards
- Accountability

U.S. Protections for Health Data

- HIPAA
  - Applies only to “covered entities” (fully) and their “business associates” (more limited)
  - Expansive definition of “protected health information” (PHI) (all forms)
  - All PHI largely treated as same re: degree of protections
  - 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'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

U.S. Laws

- In HIPAA, less reliance on individual consent
  - Substance abuse treatment data (Part 2) subject to more stringent consent requirements
  - State laws governing sensitive data types
- Covered entities control most data uses and disclosures

GDPR

- Went into effect on May 25, 2018
- Applies to data "controllers" and "processors" in the EU
  - Also applies to entities not located in the EU but who offer goods and services to EU residents or monitor the behavior of EU data subjects within the EU
- Applies to "personal data"
  - Lesser protections for "pseudonymized" data (data can no longer be attributed to a specific data subject without use of additional information)
  - Doesn't apply to data made public by the data subject
  - Doesn't apply to data from individuals no longer living

Highlights

- All processing must be “lawful”
  - Assumption is consent is required (explicit consent in the case of health information) absent a lawfully permitted purpose
  - Fewer of these than in HIPAA
- Security safeguards required - but expectations not set out in detail
- Controllers responsible for actions of processors
- Data Protection Impact Assessment (and in some cases regulatory review) required for certain high risk processing activities (for example, health data processed in large numbers)
- Also individual rights provisions (lots of press on the “right to be forgotten”/right of erasure)

- Necessary to protect vital interest of data subject (and subject incapable of consenting)
- Necessary for reasons of substantial public interest (on the basis of Union or EU Member law)
- Required for the purpose of medical treatment undertaken by health professionals
- Necessary for public health
- Necessary for scientific research, subject to appropriate safeguards
- Legitimate interests of the controller/processor (??)

GDPR Permitted Processing (examples)

GDPR & HIPAA Individual Rights

	Right to be Informed	Right to restriction of processing	Right of access/copy	Right of erasure	Right to rectification	Data portability
GDPR	Requires detailed disclosures on data practices, including info collected, purposes for processing, categories of recipients, etc.	Right to get controller to restrict processing under certain circumstances (where accuracy of data is contested; processing is unlawful, for example); required to inform downstream recipients unless this is impossible or involves disproportionate efforts	Right to know what information controller has, right to obtain copies (within 30 days; free unless request is excessive)	Aka the "right to be forgotten;" applies if no longer basis for lawful processing or other reasons; must use reasonable efforts to communicate to downstream recipients	Right to obtain rectification of inaccurate personal data (includes right to have incomplete personal data completed through supplementary statement)	Right to receive personal data in a structured, commonly used and machine readable format and the right to transmit that data to another controller without hindrance, where processing is based on consent and processing is carried out by automated means
HIPAA	Notice of Privacy Practices must cover only what entity has right to use/disclose, individual rights (like a HIPAA explanation)	Right to request restriction (no requirement to honor except w/r/t disclosure to health plans for services paid for in full out of pocket)	Right to copy (within 30 days but reasonable, cost-based fee can be charged for labor associated with making the copies)	None	Right of amendment is right to "request" amendment; however must honor individual's right to submit her version	Right to digital copy of information maintained digitally; right to copy in form and format requested if reproducible in that form/format

HIPAA & GDPR - a few observations

- Similarities:
  - Exceptions for treatment, public health, research
  - Applicable to identifiable, broadly defined health data
  - Individual right of access/copy, right to request correction (somewhat…)
  - Somewhat distinct treatment of covered entities/controllers vs. business associates/processors
  - Breach notification to data subject and regulators required
  - High penalties for noncompliance

HIPAA & GDPR - a few observations

- Differences - Numerous!
  - Overall, GDPR much less specific
  - HIPAA coverage is more limited (lots of entities collecting/maintaining/using/sharing health data fall completely out of coverage)
  - More reliant on consent (although scope of exceptions somewhat unclear)
    - Where's the P and the O?
  - More comprehensive list of individual rights, including express provisions re: individual right to data portability
  - Some ability for Member States to provide for more specific guidance, but - for the most part - single regulation for all of EU

Impact of GDPR on US

- Global companies have taken steps to implement
  - Raising the bar even for companies not required to comply?
- Will US lawmakers feel compelled to fill gaps in US law?
  - Will these efforts complement or contradict GDPR?
- Will increased attention to privacy result in greater — or less - data sharing for good?
  - Impact on efforts to achieve “interoperability”?

Individuals as the "wormhole" for data portability

- Area of agreement between HIPAA and GDPR
  - HIPAA's permissive sharing provisions are "may share" (not must) (GDPR similar)
  - In contract, entities MUST share with individuals upon request (except in rare circumstances)
    - ✓ GDPR covers under right of access & right to data portability
- Individuals have the right to digital copies of their health information, which they can then share with whomever they please

FHIR critical to individual data portability

- HIPAA access rights underutilized
  - Lack of knowledge
  - Widespread noncompliance
  - Complicated processes, high fees, still too much paper and fax machines!
- Goal: frictionless access
- Need to maintain efforts to increase scope of information required to be made available through APIs

ciitizen | we can do more. together.

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