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

Data Considerations for Precision Oncology Care: Governance and Privacy

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

Key: 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
- Informed consent/automomy is one principle – but it is not absolute
  - Others: transparency; data minimization; safeguards; accountability

Governing research uses of health data

- Heavy reliance on de-identification (or anonymization) of data
  - Consistent with data minimization principles
  - Historically has resulted in data "free" from U.S. regulation (if done appropriately)
- Otherwise, consent required – but recently U.S. regulators have allowed for more general consents for uses of identifiable data for research purposes (HIPAA guidance & Common Rule changes)

Recent privacy law trends

- More attention focused on this issue – passage of new, sweeping privacy legislation in California last summer
- Trend is toward requiring more explicit consent
  - Some recognition of potential negative impact on biomedical research
  - So allow "general" consents – but at same time, must have "sufficient detail" to inform

Recent privacy law trends (2)

- Broadening the definition of "identifiable" or "personal" data and setting a higher bar for data to be considered "de-identified"
- Increasing individual rights with respect to data (right to access and portability, right of amendment, right to restrict uses, right to withdraw consent, right to be forgotten)

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 collect information from, or monitor the behavior of , EU data subjects within the EU
- Applies to “personal data”
  - Data still regulated but some relaxation of rules (individual rights provisions) regarding “pseudonymized” or “coded” data
  - Doesn’t apply to data made public by the data subject
  - Doesn’t apply to data from individuals no longer living

GDPR

- “‘[P]ersonal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

GDPR

- No definition of "de-identified" data; in general, data falls outside of GDPR if it doesn't meet the definition of "personal data."
- In general, data is not "personal data" only if there is no reasonable means through which someone who has access to the data could use the data to re-identify an individual who is the subject of the data.
- Seems to be a higher standard than HIPAA (either safe harbor or statistical method)

Highlights

- All processing must be “lawful”
  - Assumption is consent is required (explicit consent in the case of health information) absent a lawfully permitted purpose
- Security safeguards required - but expectations not set out in detail
- 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

CCPA (goes into effect 1/1/2020)

- Applies to a "Business" that:
  - Has annual gross revenues in excess of twenty-five million dollars ($25,000,000) (*California revenue*?);
  - Alone or in combination, annually *buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more CA consumers, households, or devices*; or
  - *Derives 50 percent or more of its annual revenues from selling CA consumers' personal information.* (Emphasis Added)

CCPA covers "personal information"

"Personal Information"

- **SB 1121 1798.140**(o)
- (1) "'**Personal Information**'" means information that *identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*
- Personal *information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household*:
  - (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
  - (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
  - (C) Characteristics of protected classifications under California or federal law.
  - (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
  - (E) *Biometric information.*

CCPA "personal information"

- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- (G) Geolocation data.
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.
- (I) Professional or employment-related information.
- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- (K) *Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.* (Emphasis added)

CCPA – definition of "deidentified"

SB 1121 1798.140

- (h) **"Deidentified"** means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:
  - (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
  - (2) Has implemented business processes that specifically prohibit reidentification of the information.
  - (3) Has implemented business processes to prevent inadvertent release of deidentified information.
  - (4) Makes no attempt to reidentify the information.
- Believed to be stricter than HIPAA & Common Rule

CCPA Exemptions for Health Entities

1798.145

(c)(1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation, or pursuant to the human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of business associate," covered entity," and "protected health information" in Section 160.103 of title 45 of the Code of Federal Regulations shall apply.

Impact of GDPR (& CCPA)

- 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 or to provide a federal standard that preempts the new CA law?
  - Will these efforts complement or contradict GDPR?
- Will increased attention to privacy result in greater — or less - data sharing for good?
- Impact of services empowering individuals to gather and share their data, including health data?

ciitizen | we can do more. together.

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