COPPERSMITH
BROCKELMAN
LAWYERS

Legal Considerations -- Patient Privacy and Data Security

Ethical, Security, Governance, and Payment Issues with Digital Health Applications in Oncology

Opportunities and Challenges for Using Digital Health Applications in Oncology:
A Virtual Workshop- National Cancer Policy Forum
July 13, 2020

Kristen B. Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com
602-381-5464

Agenda

- Patient right of access to health information and to direct disclosures to third parties
- The new information blocking and interoperability rules
- Overview of privacy requirements for data sharing in treatment and research
  - Evolving standards for de-identification of genomic information

This educational presentation is not legal advice.

Please check with your attorney for legal advice applicable to your situation.

COPPERSMITH
BROCKELMAN
LAWYERS

HIPAA Patient Rights

- Patient right to access PHI in a "designated record set"
- Patient right to direct disclosures to any third party (including personal health records, digital health applications and research databases)
  - *Ciox Health, LLC v. Azar, et al.* (D.D.C. January 23, 2020): applies only to records in the electronic health record

Two New Rules

- Office of the National Coordinator for Health Information Technology (ONC) Interoperability and Information Blocking Rule
  - 85 Fed. Reg. 25642 (May 1, 2020)
- Centers for Medicare and Medicaid Services (CMS) Interoperability and Patient Access Rule
  - 85 Fed. Reg. 25510 (May 1, 2020)
- Intent of the rules:
  - To put patients in charge of their health records
  - To make patient data requests easy and inexpensive
  - To allow health care providers to move between health IT vendors and utilize health IT solutions of their choosing
  - To promote interoperability and use of electronic health records for purposes permitted by applicable law

ONC Interoperability and Information Blocking Rule - A paradigm shift for data sharing

- Information blocking is a practice that is "likely to interfere with access, exchange or use of electronic health information" (EHI) unless the practice is required by law (i.e., data sharing is prohibited by law) or falls into one of eight regulatory exceptions
- Applies to health care providers, health information exchanges (HIE)/health information networks (HIN) and health IT developers of certified health IT
- OIG may impose CMP of up to $1 million per violation for HIE/HINs and health IT developers of certified health IT; providers will be referred to the appropriate agency for "appropriate disincentives"
  - Compliance deadline: **November 2, 2020**
  - Enforcement deadline: TBD based on OIG civil monetary penalties final rule (not yet published)
    - Proposed rule: 85 Fed. Reg. 22979 (Apr. 24, 2020)

ONC Interoperability and Information Blocking Rule

- Interoperability: new technical certification criteria
  - Requires HL7® Fast Healthcare Interoperability Resources (FHIR®) Release 4 standard and several implementation specifications, including API-enabled services
  - Attestations for encryption and multi-factor authentication standards
  - Adopts United States Core Data for Interoperability (USCDI) standard

CMS Interoperability and Patient Access Rule

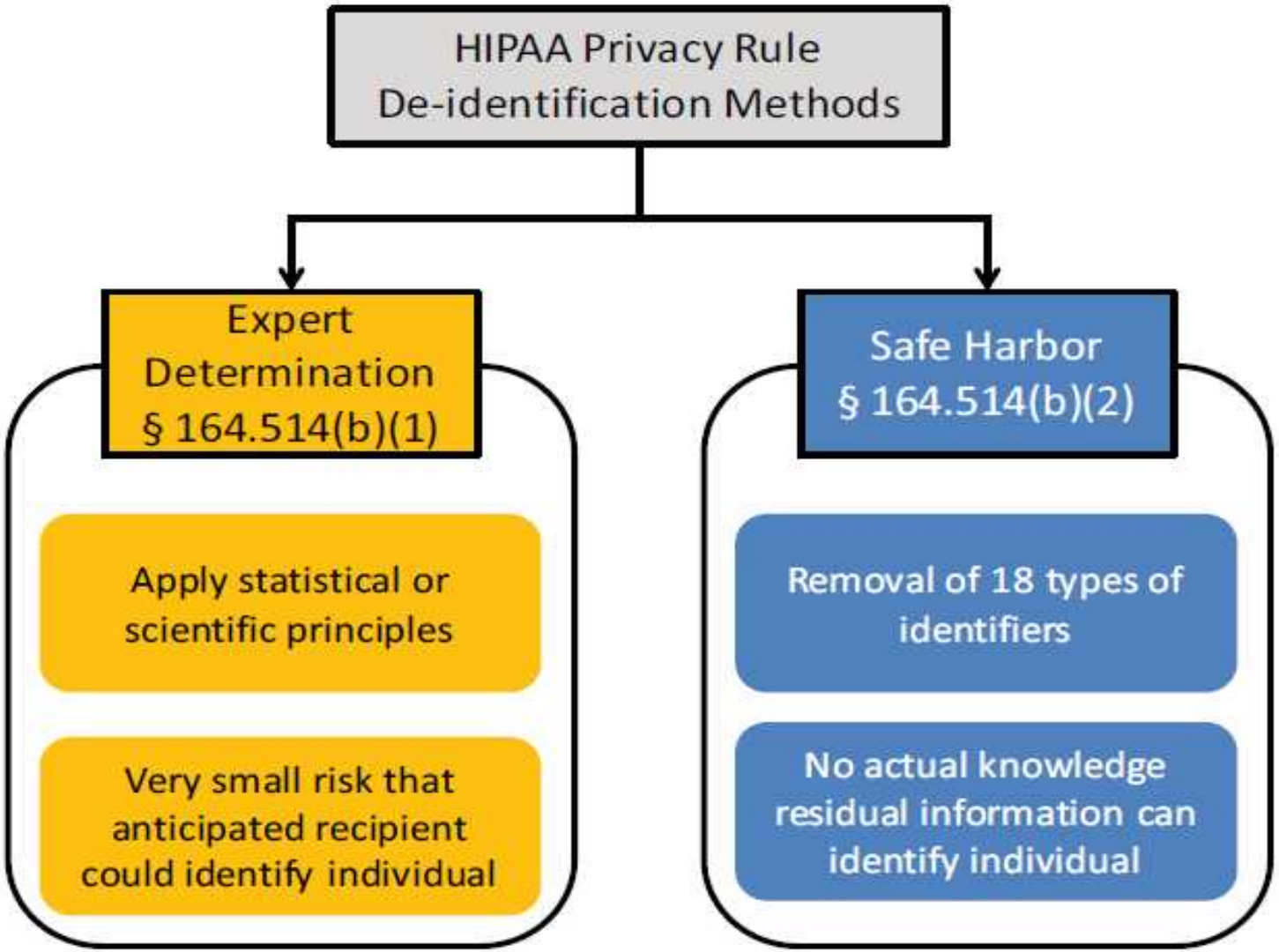
- CMS Conditions of Participation will require hospitals with EHR systems that meet the HL7 2.5.1 standard to send out inpatient and ED ADTs by **May 2, 2021**
- Patient Access API and Provider Directory API for Medicare Advantage (MA), Medicaid, and the Children's Health Insurance Program (CHIP) by **January 1, 2021**
  - Enforcement discretion until **July 1, 2021** because of COVID-19
  - Same deadline/discretion for the Patient Access API requirement for Qualified Health Plan (QHP) issuers on the individual market Federally-Facilitated Exchanges (FFEs)
- MA, Medicaid, CHIP and QHP issuers on FFE must participate in payer exchanges for care coordination by **January 1, 2022**,
- Visit CMS website for more info: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

A Complicated Web of Laws Regulating Privacy and Security in Treatment and Research

- US federal law
  - HIPAA
  - Federal substance use disorder treatment regulations (the "Part 2 regulations")
  - Common Rule
  - FDA regulations for clinical trials
  - NIH policies (the Clinical Trials Policy and regulations regarding Certificates of Confidentiality)
- US state laws
  - Consumer privacy protection laws (e.g., the California Consumer Protection Act)
  - Genetic testing laws
  - Health information confidentiality laws
  - Licensure requirements
- EU General Data Protection Regulation – and individual countries' laws throughout the world

HIPAA Privacy and Security Rules

- HIPAA Privacy Rule: a HIPAA "covered entity" (or a "business associate" on behalf of a covered entity) may disclose protected health information (PHI):
  - For treatment of a patient
  - For research if meets one of the HIPAA research rules
  - To patients and to third parties directed by patients – *more on this later*
- HIPAA Security Rule: HIPAA covered entities or business associates must have physical, administrative and technical safeguards in place to protect the security of PHI
- Standards for "de-identification" of PHI and application to genomic information

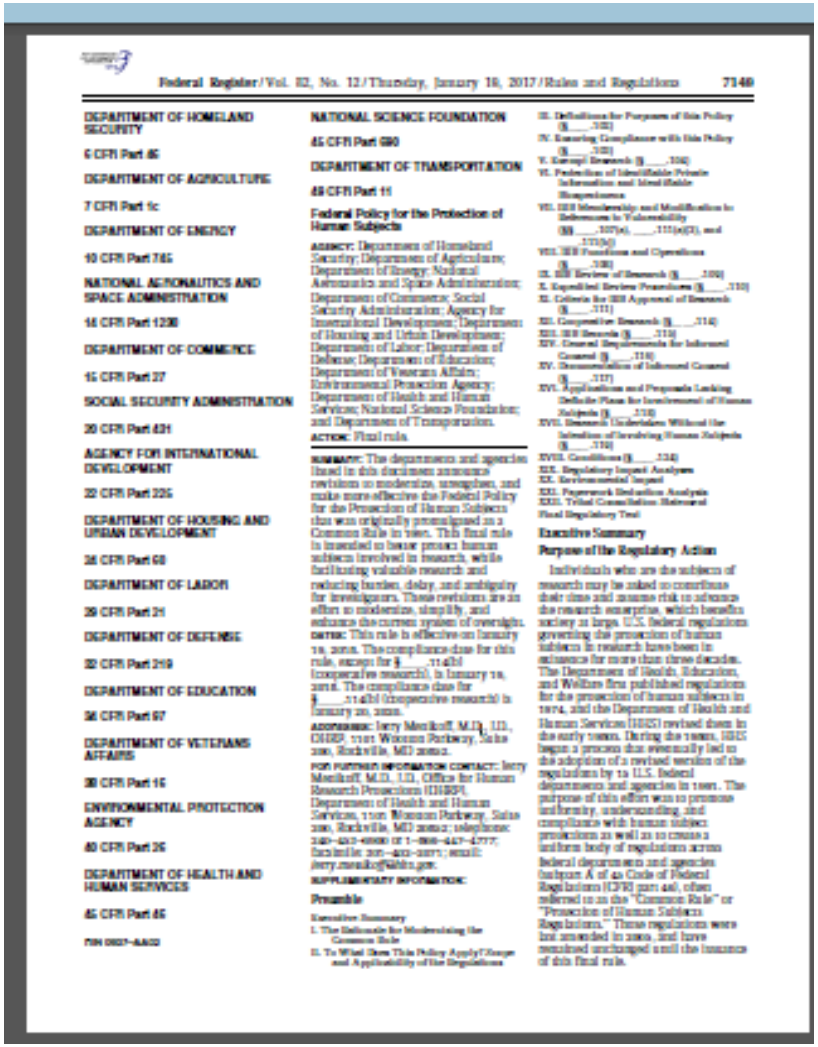


From Office for Civil Rights Guidance on De-Identification (11/25/20)
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

HIPAA: Is Genetic Information PHI?

- Genetic information is "health information"
- Health information is PHI if it is "individually identifiable information"– it identifies the individual or "there is a reasonable basis to believe the information can be used to identify the individual"
- OCR has concluded that not all genetic information is "individually identifiable," but has not provided guidance on when genetic information is individually identifiable
- Common interpretation: genetic information is not PHI unless it is accompanied by HIPAA identifiers or unless you have actual knowledge the recipient has the ability to link the genetic information to a person's identity

The Revised Common Rule



Federal Register / Vol. 82, No. 12 / Thursday, January 19, 2017 / Rules and Regulations 7149

DEPARTMENT OF HOMELAND SECURITY
6 CFR Part 46
DEPARTMENT OF AGRICULTURE
7 CFR Part 1c
DEPARTMENT OF ENERGY
10 CFR Part 745
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
14 CFR Part 1230
DEPARTMENT OF COMMERCE
15 CFR Part 27
SOCIAL SECURITY ADMINISTRATION
20 CFR Part 431
AGENCY FOR INTERNATIONAL DEVELOPMENT
22 CFR Part 225
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
24 CFR Part 60
DEPARTMENT OF LABOR
29 CFR Part 21
DEPARTMENT OF DEFENSE
32 CFR Part 219
DEPARTMENT OF EDUCATION
34 CFR Part 97
DEPARTMENT OF VETERANS AFFAIRS
38 CFR Part 16
ENVIRONMENTAL PROTECTION AGENCY
40 CFR Part 26
DEPARTMENT OF HEALTH AND HUMAN SERVICES
45 CFR Part 46
FDA 2017–N–0.

NATIONAL SCIENCE FOUNDATION
45 CFR Part 690
DEPARTMENT OF TRANSPORTATION
49 CFR Part 11

Federal Policy for the Protection of Human Subjects

AGENCY: Department of Homeland Security; Department of Agriculture; Department of Energy; National Aeronautics and Space Administration; Department of Commerce; Social Security Administration; Agency for International Development; Department of Housing and Urban Development; Department of Labor; Department of Defense; Department of Education; Department of Veterans Affairs; Environmental Protection Agency; Department of Health and Human Services; National Science Foundation; and Department of Transportation.

ACTION: Final rule.

SUMMARY: The departments and agencies listed in this document announce revisions to modernize, strengthen, and make more effective the Federal Policy for the Protection of Human Subjects that was originally promulgated as a Common Rule in 1991. This final rule is intended to better protect human subjects involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators. These revisions are an effort to modernize, simplify, and enhance the current system of oversight.

DATES: This rule is effective on January 19, 2018. The compliance date for this rule, except for §___.114(b) (cooperative research), is January 19, 2018. The compliance date for §___.114(b) (cooperative research) is January 20, 2020.

ADDRESSES: Jerry Menikoff, M.D., J.D., OHRP, 1101 Wootton Parkway, Suite 200, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT: Jerry Menikoff, M.D., J.D., Office for Human Research Protections (OHRP), Department of Health and Human Services, 1101 Wootton Parkway, Suite 200, Rockville, MD 20852; telephone: 240–453–6900 or 1–866–447–4777; facsimile: 301–402–2071; email: jerry.menikoff@hhs.gov.

SUPPLEMENTARY INFORMATION:

Preamble

Executive Summary

Purpose of the Regulatory Action

Individuals who are the subjects of research may be asked to contribute their time and assume risk to advance the research enterprise, which benefits society at large. U.S. federal regulations governing the protection of human subjects in research have been in existence for more than three decades. The Department of Health, Education, and Welfare first published regulations for the protection of human subjects in 1974, and the Department of Health and Human Services (HHS) revised them in the early 1980s. During the 1980s, HHS began a process that eventually led to the adoption of a revised version of the regulations by 15 U.S. federal departments and agencies in 1991. The purpose of this effort was to promote uniformity, understanding, and compliance with human subject protections as well as to create a uniform body of regulations across federal departments and agencies (subpart A of 45 Code of Federal Regulations (CFR) part 46, often referred to as the "Common Rule" or "Protection of Human Subjects Regulations." These regulations were last amended in 2005, and have remained unchanged until the issuance of this final rule.

- Applies to federally-funded human subjects research in the US
- Significant changes
  - **Potential changes to "identifiability"**
  - New HIPAA exemption
  - New requirements for informed consent
  - New exemption for research with "broad consent"
  - New exemption for publicly available information
  - New rule for preparing for research
  - New rule on single IRB for collaborative research

Common Rule Compliance

- Current definition of "identifiable private information": "private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information"
- "Identifiability" may change over time
  - Requires agencies to assess within one year of final rule whether there are technologies or techniques that should be considered to generate identifiable private information, even if not accompanied by traditional identifiers (such as whole genome analysis)
  - May widen difference in interpretation of "non-identified" information under Common Rule (i.e., investigator cannot readily ascertain identity of research participants) and "de-identified" under HIPAA

State Laws

- State genetic information laws
  - Some laws apply to de-identified information
  - Some laws make genetic information the "property" of the individual
  - Most laws do not distinguish between germline and somatic testing
- State consumer privacy laws having a greater impact
  - California Consumer Privacy Act (see reference slide) defines de-identified information as "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:
    - Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
    - Has implemented business processes that specifically prohibit reidentification of the information.
    - Has implemented business processes to prevent inadvertent release of deidentified information.
    - Makes no attempt to reidentify the information"
  - Pending bill to amend statute to harmonize de-identification standards with HIPAA

European Union General Data Protection Regulation (GDPR)

- Personal data directly or indirectly identifies a living person
  - Name, identification number, location data, online identifiers, factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity
- More sensitive data have special protection
  - Genetic data, biometric data for the purpose of creating unique identification, data concerning health, data regarding race, religion, politics, sex
- Treatment of de-identified data
  - No de-identification "safe harbor"– data is "anonymized" if under a "facts and circumstances" test, the data cannot be identified by any means "reasonably likely to be used … either by the controller or by another person"
  - "Pseudonymised" (coded) data still personal data if there is a link that would allow anyone to re-identify

How to Cope with Evolving Standards of De-Identification?

- Use statistical expert determination of de-identification to meet both HIPAA and evolving state de-identification standards
- Employ contractual controls over de-identified data
  - Prohibition on re-identification of individuals in data
  - Restrict downstream disclosures without approval
  - Impose specific security controls on protection of de-identified data
  - Consider location of data -- bring tools to the data (versus data to the tools) if feasible

COPPERSMITH
BROCKELMAN
LAWYERS

Reference Slides

Reference Slide: HIPAA Compliance

- HIPAA applies to "covered entities" and their "business associates"
- HIPAA applies to "protected health information" (PHI)
  - Name;
  - Street address, city, county, precinct, or zip code (unless only the first three digits of the zip code are used and the area has more than 20,000 residents);
  - The month and day of dates directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death;
  - Age if over 89 (unless aggregated into a single category of age 90 and older);
  - Certain numbers related to an individual (telephone numbers; fax numbers; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers, serial numbers, and license plate numbers; device identifiers and serial numbers);
  - Email addresses, Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses;
  - Biometric identifiers, such as fingerprints;
  - Full-face photographs and any comparable images; or
  - Any other unique identifying number, characteristic, or code

Reference Slide: HIPAA Research Rules

- The PHI is de-identified: either through removal of all HIPAA identifiers (the "safe harbor" method) or by certification of a statistical expert
- Only a "Limited Data Set" is used, subject to a "Data Use Agreement"
- The research participant or the research participant's legally authorized representative signs a written HIPAA authorization
- An institutional review board (IRB) waives or alters the HIPAA authorization requirement
- The activities are only to prepare for research, and the investigator makes certain representations
- The activities are to recruit patients to participate in clinical research (or the patients of another health care provider under a business associate arrangement)
- The research involves the information of decedents only and the investigator makes certain representations
- The research is "grandfathered" under the HIPAA rules

Reference Slide: California Consumer Privacy Act

California Consumer Privacy Act -- Cal. Civil Code 1798.100-1798.199

- Applies to any for-profit entity doing business in California that:
  - Has gross revenues above $25 million;
  - Annually buys, receives, sells or shares personal information of 50,000 or more consumers, households or devices for commercial purposes;
  - Derives 50 percent or more of its annual revenue from selling consumers' personal information
  - Affiliates of covered businesses (controls or is controlled by) and that share common branding
- Does not apply to
  - Medical information governed by the California Confidentiality of Medical Information Act (CMIA) or PHI "that is collected by a covered entity or business associate" governed by HIPAA
  - A provider governed by the CMIA or a covered entity governed by HIPAA
- Regulations at https://www.oag.ca.gov/privacy/ccpa

Reference Slide: European Union General Data Protection Regulation

- GDPR Jurisdictional reach:
  - Applies to organizations "established" (with a physician location) within the European Economic Area (EEA)
  - Applies to organizations outside the EEA that offer goods or services to data subjects within the EEA (clinical trial recruitment) or monitor the behavior of data subjects within the EEA (collection of research data from research participants)
- Applies to EEA research collaborator transfer of "personal data" to the United States
- Applies to EEA "data controller" using "data processor" outside the EEA (regardless of residency of data subject)