COPPERSMITH
BROCKELMAN
LAWYERS

Best Practices in Privacy Protection

NAS- Forum on Neuroscience and Nervous System Disorders
Neuroscience Data in the Cloud– a Workshop
September 24, 2019

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

Our Agenda

- Rosati: Overview of the complicated web of laws that apply to data sharing in research*
- Hanson and Mackay: Discussion of data sharing collaborations
- Facilitated discussion regarding:
  - Controlling for re-identification of research participants in de-identified data sets
  - Addressing challenges in obtaining consent
  - Planning for data governance in multi-institutional collaborations
- Haas: Overview of key themes and discussions

** This educational presentation is not legal advice. Please consult your legal counsel for advice on your particular circumstances.*

A Complicated Web of Laws Regulating Privacy and Security in Research

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

EU GDPR Compliance

- Applies to organizations "established" within the European Economic Area (EEA): the EU + 3 (or + 4 after Brexit)
- Applies to organizations outside the EEA that:
  - Offer goods or services to data subjects within the EEA
  - Monitor the behavior of data subjects within the EEA
- Applies to the transfer of personal data from the EEA to the US – requires legal basis for transfer:
  - Consent (and advising data subjects of the risks of transfer to the US);
  - A contract that contains model contractual clauses approved by the European Commission (which impose some GDPR requirements on receiving entity);
  - To US for-profit entities that have been certified under the EU-US "Privacy Shield"; or
  - Pursuant to codes of conduct by associations

"Personal Data" under the GDPR

- Any data that directly or indirectly identifies a living individual (not just patients)
  - 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
  - Pseudonymised (coded) still personal data – no de-identification "safe harbor" (unlike HIPAA)
  - Anonymous data (not linked)-- not personal data

When is consent required under the GDPR?

- Requires a legal basis for "processing" data
  - Consent;
  - Necessary for compliance with a legal obligation of "controller";
  - Necessary for purposes of the "legitimate interests" of the controller; or
  - Other provisions not generally relevant in the research setting
- Requires additional legal basis for processing sensitive data
  - Explicit consent;
  - Necessary for preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment;
  - Necessary for public health;
  - Necessary for scientific research; or
  - Other provisions not generally relevant in the research setting

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

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; or
- The research is "grandfathered" under the HIPAA rules.

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 2015-N-0332

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
I. The Rationale for Modernizing the Common Rule
II. To What Does This Policy Apply? Scope and Applicability of the Regulations
III. Definitions for Purposes of this Policy (§____.102)
IV. Ensuring Compliance with this Policy (§____.103)
V. Exempt Research (§____.104)
VI. Protection of Identifiable Private Information and Identifiable Biospecimens
VII. IRB Membership and Modification in Reference to Vulnerability (§§ ____.107(a), ____.111(a)(3), and ____.111(b))
VIII. IRB Functions and Operations (§____.108)
IX. IRB Review of Research (§____.109)
X. Expedited Review Procedures (§____.110)
XI. Criteria for IRB Approval of Research (§____.111)
XII. Cooperative Research (§____.114)
XIII. IRB Records (§____.115)
XIV. General Requirements for Informed Consent (§____.116)
XV. Documentation of Informed Consent (§____.117)
XVI. Applications and Proposals Lacking Definite Plans for Involvement of Human Subjects (§____.118)
XVII. Research Undertaken Without the Intention of Involving Human Subjects (§____.119)
XVIII. Conditions (§____.124)
XIX. Regulatory Impact Analysis
XX. Environmental Impact
XXI. Paperwork Reduction Analysis
XXII. Tribal Consultation Statement
Final Regulatory Text

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 years, 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 research in the US
- Effective date 1/19/19 (except for single IRB for collaborative research effective 1/20/20)
- 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

"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 identify of research participants) and "de-identified" under HIPAA

New HIPAA Exemption

- Exempts secondary research with identifiable private information or identifiable biospecimens (collected for clinical care or for a research repository), if the entity conducting the research is regulated by HIPAA
  - Will allow internal use by HIPAA covered entity (but watch "hybrid entities" like universities where the research functions are "carved out" of the HIPAA covered entity)
  - Will allow disclosure to other HIPAA covered entities (or HIPAA business associates, if for purposes of the BA's role)
  - Will not apply to biospecimens themselves, but will apply to information derived from biospecimens