COPPERSMITH
BROCKELMAN
LAWYERS

"Future Proofing" Your Activities:
Keeping up with Regulatory Developments

NAS- Forum on Neuroscience and Nervous System Disorders
Harnessing Mobile Technology to Predict, Diagnose, Monitor, and Develop Treatments for Nervous System Disorders -- June 5-6, 2018

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

A Web of Laws…

- HIPAA
- Common Rule
- FDA regulations
- NIH Policies
  - Clinical Trials Policy
  - Certificates of Confidentiality
- Federal substance abuse disorder regulations (Part 2 regulations)
- CMS and State Medicaid reimbursement regulations
- State telemedicine licensure requirements
- State health information confidentiality laws
- EU General Data Protection Regulation
- And more!

Potentially Competing Policies

- Support for advancement of research and innovation to improve care
  - 21st Century Cures Act
  - BRAIN Initiative
  - The Cancer Moonshot
  - "All of Us" Initiative
  - Etc.
- Increasing focus on individual control of data and biospecimens

HIPAA Compliance

- No regulatory changes since 2013, but lots of enforcement!
- Individuals have the right to access their own PHI in a "designated record set" or to direct release of their PHI to a third party
- HIPAA applies to "covered entities" and their "business associates"
- HIPAA applies to "protected health information" (PHI)
  - Demographic information that includes any listed "identifier"
  - Clinical and claims information without identifiers is not PHI

HIPAA Identifiers

- Data elements about individuals and their family members, household members, or employers:
  - 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

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
FOR 0937–AA02

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.

- Published final rule 1/19/17, with effective date of 1/19/18 (except for single IRB for collaborative research effective 1/20/20)
- On 1/17/18, published interim final rule delaying effective date until 7/19/18
- On 4/20/18, published proposed rule to delay effective date until 1/21/19 (but allow voluntary compliance with some provisions)

Current Status of Common Rule

- Status quo: Compliance with current (pre-2018) rule
- Institutions may voluntarily apply provisions of revised rule that do not conflict with current rule
  - *Example:* May implement revised rule's new informed consent requirements, but not revised rule's new exemptions
- Final, final rule may permit voluntary compliance with:
  - New definition of research (which lists more activities as not research)
  - No annual continuing review for certain categories of research
  - Elimination of IRB review of grant applications

Overview of Upcoming Changes to the Common Rule

- Potential changes to "identifiability" over time
- New exemption for HIPAA covered entities
- 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 whether there are technologies or techniques that should be considered to generate identifiable private information (such as whole genome analysis)
- May widen difference in interpretation of "non-identified" under Common Rule and "de-identified" under HIPAA
  - HIPAA: Genomic information is not treated as PHI unless it is accompanied by listed HIPAA identifiers

New HIPAA Exemption

- Exempts secondary research with identifiable private information or identifiable biospecimens (collected for clinical care or for a research repository), if 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
  - Will not apply to biospecimens themselves, but will apply to information derived from biospecimens

Significant Changes Coming to Informed Consent

- Include explanations:
  - That information or biospecimens will be stripped of identifiers and used without consent for future research OR that de-identified information or biospecimens will not be used for future research
  - Whether biospecimens (even if de-identified) will be used for commercial profit (and whether individual will share in the profit)
  - Whether clinically relevant results will be returned to individual
  - Whether research involving biospecimens might include whole genome sequencing

"Broad Consent"

- General consensus that will not be useful:
  - Used only for storage, maintenance, and secondary use of identifiable private information or biospecimens
  - Alternative to "regular" informed consent – broad consent is not required for secondary research
  - More requirements than "regular" consent – including that if a subject declines broad consent, you can't ask an IRB to waive consent
    - Unclear what it means to "decline" broad consent
    - Will require substantial tracking and auditing
    - Unclear how applies to downstream use of data

What Else Is Ahead in US Law?

21st Century Cures Act Implementation:

Research Policy Board

- Tasked with making recommendations for modifying and harmonizing policies and regulations across research funding agencies to minimize administrative burden
- Statutory deadline for creation of Board: December 13th, 2017 - the anniversary of 21st Century Cures

European Union General Data Protection Regulation

- New EU data protection law, effective May 25, 2018
- Applies to organizations "established" within the European Economic Area (EEA): the EU + 3
- Applies to organizations outside the EEA that:
  - Offer goods or services to data subjects within the EEA (whether or not payment required)
  - Monitor the behavior of data subjects within the EEA

"Personal Data"

- Any data that directly or indirectly identifies a living individual (not just patients)
  - Name, identification number, location data, online identifier, 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"
  - Anonymous data not personal data

Concerns with GDPR Application to Clinical Research in US

- Undue extraterritorial application to US citizens traveling to EU
- *Specific* consent for future research may be required
  - Secondary use of non-anonymized data without consent (with IRB waiver) may not be permitted
- Conflicts with EMA policies that require sponsors to make publicly available individual subject-level data for clinical trials whose results submitted to the EMA to support marketing applications
- Conflicts with NIH data sharing requirements
- May require deletion or anonymization of personal data on withdrawal of consent

What if GDPR Applies to You?

- Extensive individual rights with private right of action
- Data controller responsibilities
  - Technical safeguards
  - Policies
  - Notice of data breaches within 72 hours
  - Data protection "impact assessments" if high risk to individuals
  - Designation of data protection officer
  - Etc.

- *BIG PENALTIES – UP TO 20 MILLION EUROS or 4% annual turnover*

Pulling This All Together…

How do you "future proof" your research to ensure ability to use data collected for future research?

- Good consent processes:
  - Build in permission to use data for future research in as detailed and broad a manner as feasible
  - Build in consent for future contact
- Consider carefully what role US institution will play in a research collaboration involving organizations in the EEA and what data the US institution will receive

COPPERSMITH BROCKELMAN

LAWYERS

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

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