COSMOS
Navigate the Compliance Universe

Compliance Today - May 2022
Data governance: Unlocking data to advance research while safeguarding human subjects

By Mark J. Fox, Thora A. Johnson, and Deborah A. Marko Koeberer

Mark J. Fox (mfox@acc.org) is Privacy and Research Compliance Officer at American College of Cardiology Foundation, Washington, DC. **Thora A. Johnson** (thora.johnson@orrick.com) is Partner at Orrick, Herrington & Sutcliffe LLP, Washington, DC. **Deborah A. Marko Koeberer** (deborah.markokoeberer@uhhospitals.org) is Director, Facility Compliance, Privacy, Compliance Operations at University Hospitals Health System (Cleveland), Shaker Heights, OH.

Mark J. Fox

Thora A. Johnson

Deborah A. Marko Koeberer

Regulations governing the use of data across the healthcare ecosystem continue to evolve to catch up with technological advances that enable researchers to use and exchange data to gain valuable insights. Recent revisions to 45 C.F.R. Part 46 Subpart A (the Common Rule) and the implementation of new interoperability rules under the 21st Century Cures Act have removed barriers that previously existed to the use of health-related data in research while protecting the right of individuals to keep their health information confidential and secure. In this piece, we provide background on these changes and explain how they can be leveraged by organizations to expand the responsible use of data in research settings. We then explore how organizations engaged in these activities can promote good data stewardship by implementing the fundamental principles of an institutional data governance structure.

Revised Common Rule

The Common Rule establishes the boundaries by which investigators may perform research while protecting the rights of human subjects. The Common Rule was revised in January 2017 in order to strengthen the protections for study participants while limiting burdensome administrative obligations for researchers.[1]

Prior to the introduction of the revised rule, there remained a large gap in how to address the secondary use of data in the performance of human subject research. The revised Common Rule included a number of changes to provide additional clarity on this use of data. For example, the revised Common Rule updated the definition of human subject to "a living individual about whom an investigator (whether professional or student) conducting research…obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or…obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens."[2] This further clarified the inclusion of data and biospecimens.

In addition, several of the exemptions under the Common Rule were revised. Of particular note is Exemption 4, which applies to the secondary research use of identifiable private information or identifiable biospecimens. The revision to Exemption 4 expanded the applicability of the exemption to secondary research using identifiable private information if the research only covers the collection and analysis of identifiable information regulated

under the Health Insurance Portability and Accountability Act (HIPAA) as "health care operations," "research," or "public health activities and purposes."[3] (Note that secondary research is defined as research with materials originally obtained for nonresearch purposes or for research other than the current research proposal.) Under this exemption, informed consent from research subjects is not required for institutions that are either a covered entity or business associate under HIPAA and fully comply with the HIPAA Security Rule. This provides covered institutions with the ability to conduct secondary research with less regulatory burden.

Another concept under the revised Common Rule is broad consent. Exemption 7 of the revised Common Rule permits the use of broad consent for the storage or maintenance of identifiable private information or identifiable biospecimens for secondary research with limited institutional review board (IRB) review.[4]

There are six additional elements of broad consent that must be included in the consent form.[5] These elements include:[6]

> 2. A general description of the types of research that may be conducted with the identifiable private information or identifiable biospecimens. This description must include sufficient information such that a reasonable person would expect that the broad consent would permit the types of research conducted;
>
> 3. A description of the identifiable private information or identifiable biospecimens that might be used in research, whether sharing of identifiable private information or identifiable biospecimens might occur, and the types of institutions or researchers that might conduct research with the identifiable private information or identifiable biospecimens;
>
> 4. A description of the period of time that the identifiable private information or identifiable biospecimens may be stored and maintained (which period of time could be indefinite), and a description of the period of time that the identifiable private information or identifiable biospecimens may be used for research purposes (which period of time could be indefinite);
>
> 5. Unless the subject or legally authorized representative will be provided details about specific research studies, a statement that they will not be informed of the details of any specific research studies that might be conducted using the subject's identifiable private information or identifiable biospecimens, including the purposes of the research, and that they might have chosen not to consent to some of those specific research studies;
>
> 6. Unless it is known that clinically relevant research results, including individual research results, will be disclosed to the subject in all circumstances, a statement that such results may not be disclosed to the subject; and
>
> 7. An explanation of whom to contact for answers to questions about the subject's rights and about storage and use of the subject's identifiable private information or identifiable biospecimens, and whom to contact in

> the event of a research-related harm.

The concept of broad consent is new, and many institutions are still struggling to determine its feasibility.

Complementing broad consent are revisions imposed by the HIPAA Omnibus Rule, which removed significant barriers to secondary research by allowing "compound authorizations."[7] These authorizations allow researchers to combine "conditioned" and "unconditioned" uses of protected health information. One example is to combine an authorization for a clinical trial with an authorization to use data in a central data repository. Note that both conditioned and unconditioned uses must be clearly outlined with an opportunity to opt out of unconditioned uses.

The revised Common Rule does not impose privacy and security obligations as proposed in the initial notice of proposed rulemaking but does require the development of additional guidance on privacy and security safeguards.[8] Even in the absence of additional guidance, IRBs continue to have a role in appropriately safeguarding research studies. As organizations evaluate appropriate protocols, they should consider the following questions:

1. Does your IRB provide specific guidance on safeguarding private health information?
2. Has your institution developed research-specific guidance and policies on protecting the privacy and security of research data?

21st Century Cures Act: Information blocking rules

The 21st Century Cures Act,[9] signed into law on December 13, 2016, passed overwhelmingly in both the U.S. House of Representative and Senate following a multiyear bipartisan effort to accelerate the pace of the discovery, development, and delivery of new treatments and cures. The 21st Century Cures Act provides $6.3 billion in funding for a variety of purposes, including streamlining the U.S. Food and Drug Administration's processes for drug and medical device approvals, addressing the nation's opioid crisis, funding new National Institutes of Health research on human genetics and control over medical records, reforming the delivery of mental health and substance abuse prevention and treatment, and facilitating secure and interoperable exchange of electronic health record data while protecting patients' privacy.

The relevant and key provision of the 21st Century Cures Act focuses on adopting standards that promote the interoperability of health information, thereby providing individuals more control and access to their own health data without "special effort."[10] Interoperability, as defined by the 21st Century Cures Act, means health information technology that "enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user," allowing "for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law."[11]

To further enable interoperability, the 21st Century Cures Act prohibits "information blocking," a practice by a health IT developer, health information network (HIN), health information exchange (HIE), or healthcare provider that, except as required by law or specified by the secretary of the U.S. Department of Health & Human Services (HHS), is likely to interfere with access, exchange, or use of electronic health information (EHI).[12]

Information blocking practices may include:[13]

A. Practices that restrict authorized access, exchange, or use under applicable State or Federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies;

B. Implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information; and

C. Implementing health information technology in ways that are likely to—

   i. Restrict the access, exchange, or use of electronic health information with respect to exporting complete information sets or in transitioning between health information technology systems; or

   ii. Lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health information technology.

In addition, the 21st Century Cures Act directs the secretary of HHS to establish a prohibition on any action that constitutes information blocking as a requirement for obtaining and maintaining health IT certification under the Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification Program.[14]

EHI is defined as the electronic protected health information in a designated record set (as defined by HIPAA) regardless of whether the records are used or maintained by or for an entity governed by HIPAA.[15] EHI specifically excludes psychotherapy notes (as defined under HIPAA) as well as "information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding." However, there is an important transition rule. Specifically, until October 6, 2022, for the purposes of the information blocking definition, EHI is limited to the data elements represented in the USCDI V1 standard adopted in the final rule.[16]

The ONC final rule[17] establishes eight categories of practices that **do not** constitute information blocking exceptions:

- "Exceptions that involve not fulfilling requests to access, exchange, or use EHI":
  - **Preventing harm exception**: It is not considered information blocking if an actor engages in practices with the "reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information."[18]
  - **Privacy exception**: It is not considered information blocking if an actor does not fulfill "a request to access, exchange, or use electronic health information in order to protect an individual's privacy," provided certain conditions are met.[19]
  - **Security exception**: It is not considered information blocking for an actor "to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic

health information," provided certain conditions are met.[20]

- **Infeasibility exception**: It will not be information blocking if an actor does not fulfill "a request to access, exchange, or use electronic health information due to the infeasibility of the request," provided certain conditions are met.[21]
- **Health IT performance exception**: It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.[22]

- "Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI":
  - **Content and manner exception**: It is not information blocking for an actor to limit "the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information," provided certain conditions are met.[23]
  - **Fees exception**: Is it not considered information blocking under the fees exception if a covered component charges "fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using electronic health information," provided certain conditions are met.[24]
  - **Licensing exception**: It is not information blocking for an actor "to license interoperability elements for electronic health information to be accessed, exchanged, or used," provided certain conditions are met.[25]

Information blocking can pose a threat not only to patient safety, but also undermine the efforts of providers, payers, and others to create a more efficient and effective healthcare system. Under the 21st Century Cures Act, the HHS Office of Inspector General (OIG) is authorized to investigate information blocking claims against actors, and the HHS secretary to enforce civil monetary penalties.

For health IT developers of certified health IT, HIEs, and HINs, the OIG is currently engaged in rulemaking to establish enforcement dates. On April 24, 2020, OIG introduced a proposed rule regarding information blocking civil monetary penalties and explaining OIG's anticipated approach to enforcement and coordination within HHS to implement the information blocking authorities.[26] OIG explains that it will likely focus its enforcement efforts on "conduct that: (i) resulted in, is causing, or had the potential to cause patient harm; (ii) significantly impacted a provider's ability to care for patients; (iii) was of long duration; (iv) caused financial loss to Federal health care programs, or other government or private entities; or (v) was performed with actual knowledge."[27] OIG emphasized in its proposed rule that it would "closely coordinate with ONC" on information blocking enforcement. The proposed rule would incorporate statutory changes in three areas:

1. Condition and maintenance of certification requirement enforced by ONC (applicable to health IT developers of certified health IT);
2. Civil monetary penalties of up to $1 million per violation imposed by the OIG (applicable to health IT developers of certified health IT, HIEs, and HINs); and
3. Appropriate government agency disincentives, to be defined through future notice-and-comment rulemaking (applicable to healthcare providers).

For healthcare providers, the OIG has yet to propose an enforcement mechanism—however, healthcare providers that meet the definition of a health information exchange or health information network are subject to information blocking civil monetary penalties. While healthcare providers are not subject to the $1 million per violation penalty, the OIG will instead refer matters of information blocking to the appropriate agency to be subject to appropriate disincentives using authorities under applicable federal law, as HHS "sets forth through notice and comment rulemaking."[28] Moreover, the names of healthcare providers who indicate "no" responses to certain prevention of information blocking statements tied to Medicare reimbursement will be published.[29]

The interoperability rules advance health IT infrastructure that supports research, improves data quality at the point of capture, and increases data harmonization and access, and expands the number of health-related data sources.

Data governance

Data governance provides a framework to protect, secure, and accurately gather each piece of data an organization possesses. Governance of clinical data is extremely important for research as it enables an organization to maximize its visibility into the data in its possession. Data governance makes it possible for researchers to have direct access to high-quality data that is clearly defined and unlock the clinical research potential of the data an organization possesses.

Establishing a prescribed data governance structure is important to ensure data is accessible, usable, and protected. An effective data governance structure clearly defines where the data is, and who has authority and control over it. A data governance structure looks at both the data itself and the people, processes, and technology necessary to manage and protect this critical healthcare asset. Successfully implementing data governance enables rapid access to data that is permitted, readily available, easy to use, well defined, and high quality.

A strong data governance program is built on 1) knowing where the data lives, 2) understanding how the data moves around the environment, 3) creating risk profiles for the data and reviewing privileges to the data, and 4) creating a data governance team. Think about this for a moment: Do you *really* know where all your data resides, or do you have a "pretty good" idea of where everything is? A strong data governance program will ensure that an organization knows the answer and understands how data moves around the organization. It will unlock data for clinical researchers to ask questions and have results at their fingertips. It's important to note that as an organization works through its data governance journey, it will also define privileges to the data. Aggregated results or deidentified data may be immediately available to researchers, but anyone requiring identifiable data would need to obtain IRB approval, as prescribed in the Common Rule.

Within this framework, there are many ways that an organization can set up a data governance structure. For example, it can begin by establishing a data governance council that will define the road map for the program and set the priorities for the foundation of the program. Executive buy-in at this level is important to drive and support the program as it is initiated and matures and evolves over time. In addition to executive support, a data governance office will manage implementation of the road map and day-to-day activities. Members of the data governance office should have a keen understanding of why data governance is important to your organization, strong project management skills, and be technically proficient to support technology solutions.

The data governance council will identify information owners. Information owners understand the business function of the data and make decisions about the collection, movement, access, and use of the data for specific data domains across all applications and the business units. The more data an organization has, the more information owners will be necessary to manage the various data domains. Information owners will ensure the

same data collected in various systems or through different methods are normalized and harmonized. They will work closely with data stewards, application stewards, and analytics stewards to ensure the data is understood and made accessible to everyone within the privileges defined for each data element.

Example data governance structure

1. Data governance council
    a. Sets program priorities and defines road map.
2. Data governance office
    a. Coordinates program activities, implements and manages technology solutions.
3. Information owner
    a. Makes data collection, movement, archiving, access, and use decisions for specific data domains across all applications and business units.
4. Data steward
    a. Provides local data use expertise.
5. Application steward
    a. Provides application- and data source–specific expertise.
6. Analytics steward
    a. Represents a team of individuals who create and distribute information.

Takeaways

- Prior to the introduction of the revised Common Rule, there was a large gap in how to address the secondary use of data in the performance of human subject research.
- Changes to both HIPAA and the Common Rule harmonized privacy protections with human subject protection regulations.
- The interoperability rules advance health IT infrastructure that supports research, improves data quality at the point of capture, increases data harmonization and access, and expands the number of health-related data sources available to an organization.
- Data governance provides a framework to protect, secure, and accurately gather each piece of data an organization possesses.
- Implementing a data governance structure can enable organizations to unlock the clinical research potential of the data in their possession.

1 "Revised Common Rule," U.S. Department of Health & Human Services, last reviewed January 19, 2017, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html.
245 C.F.R. § 46.102(e)(1) .
345 C.F.R. § 46.104(d)(4)(iii) .

445 C.F.R. § 46.104(d)(7) .
545 C.F.R. §§ 46.104(d)(7), 46.111(a)(8) .
645 C.F.R. § 46.116(d)(2)–(7) .
745 C.F.R. § 164.508(b)(3) .
8 Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7,149, 7,202 (January 19, 2017) .
9 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).
1045 C.F.R. § 170.404(a)(1) .
11 21st Century Cures Act § 4003, 130 Stat. 1165.
12 21st Century Cures Act § 4004, 130 Stat. 1176.
1342 U.S.C. § 300jj-52(a)(2) .
1442 U.S.C. § 300jj-11(c)(5)(D)(i) .
1545 C.F.R. § 171.102 .
16 Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency, 85 Fed. Reg. 70,064, 70,069 (November 4, 2020) .
17 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642 (May 1, 2020) .
1845 C.F.R. § 171.201 .
1945 C.F.R. § 171.202 .
2045 C.F.R. § 171.203 .
2145 C.F.R. § 171.204 .
2245 C.F.R. § 171.205 .
2345 C.F.R. § 171.301 .
2445 C.F.R. § 171.302 .
2545 C.F.R. § 171.303 .
26 Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22,979 (April 24, 2020) .
27 Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22,984 .
2842 U.S.C. § 300jj-52(b)(2)(B) .
29 Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers, 85 Fed. Reg. 25,510, 25,575 (May 1, 2020) .