COSMOS
Navigate the Compliance Universe

Research Compliance Professional's Handbook, Third Edition
8 Research Privacy and Security: Myths, Facts, and Practical Approaches

By Marti Arvin, JD, CCEP-F,CHC-F,CHPC,CHRC, Kathleen Price, RN, MBA, CIP, and David Vulcano, LCSW, MBA, CIP, RAC[1]

Introduction

An individual's right to privacy has been a well-established principle in the American healthcare system for a long time. A healthcare provider or researcher has an obligation to protect the confidentiality of a patient's or subject's identifiable private information against unauthorized use or disclosure. These principles have deep historical roots. Indeed, a physician's duty to treat as confidential any information gained when caring for a patient dates back to around the time of the Greek philosophers,[2] and is well-ensconced in Anglo-American law and jurisprudence.[3] It is also one of the general principles articulated in the Declaration of Helsinki: "It is the duty of the physician in medical research to protect the life, health, privacy, and dignity of the human subject."[4]

This chapter includes descriptions of federal and state privacy, confidentiality, and security laws and regulations that govern clinical research in the United States, as well as practical recommendations for compliance consistent with the efficient conduct of that research.

Federal Privacy Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations[5] are perhaps the best-known federal privacy rules today. The Common Rule,[6] corresponding FDA regulations, [7] and other federal laws and regulations also protect the privacy and confidentiality of records created, used, and disclosed in human research. These federal mandates are discussed below.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Congress enacted HIPAA in 1996 to assure individuals the ability to move from one job to another without risking their health insurance coverage and to strengthen federal fraud and abuse laws. The law included "administrative simplification" provisions designed to encourage standardization of health insurance claims submission and processing and to promote overall efficiency in the healthcare system.[8] Recognizing that standardization would facilitate electronic storage and transmission of health information, and concerned that a move to use of electronic records would increase risks to health privacy, Congress included privacy protection provisions and a mandate that, absent further legislative action, the Secretary of Health and Human Services would develop and implement regulations to protect individually identifiable health information.[9] Those regulations were released as a "final rule" in December 2000[10] and the HIPAA Privacy Rule became effective in April 2003.

The HIPAA Omnibus (Final) Rule

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

In 2013 the Department of Health and Human Services (HHS) released the "Omnibus Rule," which resulted in modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules.[11] HHS published the Omnibus Rule, also known as the Final Rule, in January and it went into effect on March 26, 2013. Covered entities and business associates were required to be in compliance with most of the directives in the rule since September 23, 2013.

The Omnibus Rule implements most of the privacy and security provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The rule provides for increased focus on patient rights and providing health information to patients. Restrictions on some uses and disclosures of protected health information (*e.g.*, sale of PHI, marketing, fundraising limitations, and allowance for patient out-of-pocket payment without notification of payers) are included. The rule extends the provisions of the Security Rule to business associates and subcontractors.

Changes in the Enforcement Rule altered HIPAA enforcement from a program with very little punitive power to a more substantive penalty-based system. The penalties range from $100–$50,000 per violation, with a $1.5 million cap per calendar year for all violations of an identical provision, and criminal penalties of up to 10 years' imprisonment. Where there is a possibility of a violation occurring due to willful neglect, HHS can impose civil monetary penalties in the higher ranges of $10,000–$50,000 per violation per provisions.

Uses and disclosures of PHI for research purposes are included in 45 C.F.R. § 164.512 , Standard (i) of the regulations, "Uses and disclosures for which an authorization or opportunity to agree or object is not required." This section describes the waiver process, IRB and privacy board requirements, and reviews preparatory to research and review and approval procedures.

The Omnibus Rule removed significant barriers to clinical research and provided more flexibility for future research endeavors. Authorizations for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or for another research study. Previously, a participant in a clinical trial could only authorize the use of PHI for one clinical trial per authorization. The Privacy Rule prohibited combining an authorization that conditioned treatment, payment, enrollment in a health plan, or eligibility for benefits (i.e., a conditioned authorization) with an authorization for another purpose for which treatment, payment, enrollment, or eligibility might not be conditioned (i.e., an unconditioned authorization). Thus, prior to the Omnibus Rule, a covered entity could not, for example, combine an authorization to use and disclose PHI for research in connection with a clinical trial (which is a conditioned authorization) with an authorization to create a central research repository or tissue bank for future research (which might be an unconditioned authorization). Authorizations for unspecified future research were prohibited.

The Omnibus Rule harmonizes authorization requirements with federal human subject protection rules, and permits the use of compound authorizations, combining conditioned and unconditioned authorizations, and permitting the use or disclosure of PHI for future, unspecified research. Thus, a single document that includes consent and authorization for a clinical trial and a future study, as long as the authorization includes a general description of the types of research that might be conducted, can now be used. The authorization must clearly differentiate between conditioned and unconditioned authorizations for research and provide the individual with the option to opt in to the unconditioned research activities. The change to compound authorizations will simplify the administration of clinical trials and facilitate outcomes research involving tissue and data banking information.

The use of compound authorizations requires covered entities to revise authorization processes and forms, including the process for future revocations by subjects.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Authorization for use or disclosure of psychotherapy notes continue to have the restriction that the form may only be combined with another authorization for use or disclosure of psychotherapy notes, and may not be combined with other authorizations.

Prior to enactment of the Omnibus Rule, authorization for research had to be study-specific. The change provides that a valid authorization can be used for future research studies and will benefit secondary research efforts. Future research need not be related to a current study, as long as the authorization adequately describes potential future research in a way that it would be reasonable for the subject to expect that PHI could be used or disclosed for the research.

In the Omnibus Rule, HHS also confirmed that researchers may be business associates if they perform a service for covered entities, *e.g.*, de-identifying PHI or creating a limited data set, even if the de-identified PHI or limited data set is created for use by the researcher—provided there is separation between the business associate activity of creating the data set and the activity of performing the research. As stated in the Rule:

> However, a researcher may be a business associate if the researcher performs a function, activity, or service for a covered entity that does fall within the definition of business associate, such as the health care operations function of creating a de-identified or limited data set for the covered entity. See paragraph (6)(v) of the definition of ''health care operations.'' Where the researcher is also the intended recipient of the de-identified data or limited data set, the researcher must return or destroy the identifiers at the time the business associate relationship to create the data set terminates and the researcher now wishes to use the deidentified data or limited data set (subject to a data use agreement) for a research purpose.[12]

Although HIPAA does not directly govern research, its privacy and security rules do regulate healthcare providers, health plans, and clearinghouses (collectively "covered entities"[13] that often control data researchers need to conduct clinical studies). Moreover, HIPAA violations may result in significant penalties ranging from small assessments per violation up to 10 years' imprisonment and multi-million dollar fines in the most egregious cases,[14] not to mention negative publicity and loss of public trust. As a result, some covered entities have adopted very conservative—and sometimes unnecessarily restrictive—approaches to data sharing that hinder good clinical research.[15] A strong grasp of the legal and regulatory requirements that govern privacy, confidentiality, security, and data sharing can help researchers, IRBs, and privacy officers avoid this problem.

1. Basic Privacy Rights

Under the Privacy Rule, as it is known, a covered entity may not use or disclose an individual's PHI unless the use or disclosure is authorized in writing by the individual (or his or her personal representative[16]), or a specified regulatory exception applies.[17] These exceptions are described in detail in subsection below. To be valid, an authorization to use or disclose PHI for research must include the following elements and statements:[18]

- A description of the study (*e.g.*,the title and purpose)
- A description of any PHI to be used or disclosed for the study
- The names or groups of persons involved in the research (*e.g.*, "researchers and their staff")

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

- A statement thatthe subject's PHI may not be protected under HIPAA once it is disclosed outside the covered entity
- A statement either that: (i) authorization is voluntary, but failure to agree to the requested use or disclosure will bar the prospective subject from participating in the study (for any research conducted by a covered entity that involves treatment); or (ii) participation is voluntary and the covered entity may not condition testing or treatment on whether the prospective subject signs the authorization (for research that does not involve research-related treatment)
- Information about withdrawal
- Information regarding future revocation, when a compound authorization is used
- Expiration date or event (a date may be given, or an event such as "the end of the study,"); researchers may extend authorizations indefinitely by explicitly stating that there is no expiration date
- Signature of subject or subject's personal representative
- Date of signature

The Privacy Rule identifies essential privacy rights and requires covered entities to develop and implement policies and procedures designed to protect those rights. For a complete listing and information regarding these rights, refer to the 45 C.F.R. Part 164, Subpart E, "Privacy of Individually Identifiable Health Information." Key privacy rights described in Subpart E include rights to the following.

Notification of a Covered Entity's Privacy Practices [19]

The Privacy Rule requires covered entities to provide written notice of their privacy practices to individual patients or health plan members, to post those notices on their public websites, and to promptly publish information about material changes. A covered entity may provide the notice to an individual by Email, if the individual agrees to electronic notice and such agreement has not been withdrawn. The notices must inform individuals of the circumstances under which their PHI may be used without their permission including, if applicable, for research or public health activities.

The Omnibus Rule requires that covered entities revise the notice of privacy practices to include the following:

a. Prohibition against health plans using or disclosing genetic information for underwriting purposes;
b. Prohibition on the sale of PHI without the express written authorization of the individual, and other uses and disclosures that expressly require the individual's authorization (marketing and disclosure of psychotherapy notes);
c. Duty of a covered entity to notify affected individuals of a breach involving their PHI;
d. Individual's right to opt out of receiving fundraising communications for entities that have stated their intent to fundraise in the notice of privacy practices; and
e. Individual's right to restrict disclosures of PHI to a health plan where the individual pays out of pocket in full for the service.

Inspect and Copy Healthcare Records[20]

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

The Privacy Rule defines a "designated record set" (DRS) to include medical and billing records, as well as other records used to make decisions about individuals, and requires covered entities to maintain DRS records for at least six years and make those records available to the individuals to whom they pertain.[21] Because the definition of a DRS is broad, it extends to clinical research records created, received, or maintained by a covered entity, even if solely for research purposes and even if they involve only "research subjects" and not "patients."

Access of Individuals to Protected Health Information

Individuals have a right to request copies of their own PHI in any form they choose, including electronic copies, provided the PHI is "readily producible" in that format. Covered entities must provide copies of PHI to other parties as designated by the individual, based upon a written and signed request that clearly identifies the designated recipient and where to send the copy of PHI. Of note, however, HIPAA allows the covered entity to withhold the release of certain research related information for a period of time if the patient agreed to it up front as part of their signed authorization. This would be important in studies that require blinding of the participants for scientific purposes. All requests for access must be addressed (granted or denied) within 30 days. Covered entities may also be permitted a one-time 30-day extension by providing notice to the individual of the reasons for the delay.

Covered entities must permit individuals to request their records and must accommodate reasonable requests by individuals to receive communications of PHI by alternative means or at alternate locations. Covered entities may send individuals unencrypted Emails including electronic protected health information (ePHI), if the individual requests it, provided that the covered entity has advised the individual of the risk and the individual accepts that the message will be delivered via unencrypted email.

Amendment of Protected Health Information[22]

An individual has the right to have a covered entity amend PHI or a record about the individual in a DRS for as long as the PHI is maintained in the DRS. The covered entity may deny the request for amendment, if it determines that the PHI or record was not created by the covered entity, is not part of the DRS, would not be available for inspection, or is accurate and complete. The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of the request. The covered entity may extend the time for action by no more than 30 days provided that the individual is provided with a written statement about the reasons for the delay and the date by which the covered entity will complete its action on the request. The covered entity must maintain information about any objections.

Receive an Accounting of Certain Unauthorized Disclosures[23]

The Privacy Rule requires covered entities to maintain records of certain disclosures done without written authorization, including disclosures for public health purposes and for research conducted pursuant to a waiver of authorization by an Institutional Review Board (IRB) or Privacy Board, reviews preparatory to research and research on decedent information. The covered entity must provide information about those disclosures to patients upon request.

This list must be tied to each disclosure of the identifiable record and must contain, among other things, the name(s) and address of the accessing researchers and the date and the purpose of the access (*i.e.*, the title of the research activity). If, however, the researcher accesses more than 50 identifiable records for that research activity, the covered entity may, in lieu of tagging each identifiable record disclosed, keep a master list of such projects. This abbreviated list requires information additional to that of the above, such as the name and phone

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

number of the sponsor. When utilizing the abbreviated listing for documenting more than 50 records accessed, that list would be given to all patients whose records might have been accessed in addition to the list of the known accesses. Specifically, when a patient asks the covered entity for their accounting of disclosures, the covered entity would provide the list of the activities of known access of that patients record as well as the master list of which their record might have been accessed when not documenting it individually.

2. Authorization Exceptions

The Privacy Rule permits use or disclosure of PHI without an individual's written authorization for "treatment," "payment," and "healthcare operations" (TPO). These terms do not include most research activities.[24] HIPAA also permits use or disclosure to law enforcement and public health authorities, subject to specified limitations.[25]

HIPAA includes five additional exceptions to the written authorization requirement relevant to research activities, which are described below.

Waiver of Authorization[26]

The Privacy Rule empowers an institutional review board (IRB) whose membership meets the membership criteria under the Common Rule, or a properly constituted privacy board, to grant a waiver or alteration of written authorization if the proposed use or disclosure will pose minimal risk to participants' privacy and other specified criteria are met. A comparison of Common Rule and HIPAA waivers and detailed discussion of the role of a privacy board under HIPAA is discussed later in this chapter. Of note, although there is overlap in the criteria for this waiver of authorization and the waiver of obtaining informed consent to be in the research, these are separate and distinct decisions the IRB must make and document separately.

Review Preparatory to Research[27]

A covered entity may allow researchers, whether or not affiliated with the covered entity, to review PHI without written authorization from affected individuals if the researchers certify that: (1) the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; (2) no PHI will be removed from the covered entity by the researcher in the course of the review; and (3) the PHI for which use or access is sought is necessary for the research purposes.

Through its FAQ process, the Office of Civil Rights clarified that this exception could be used to permit individuals to identify potential research subjects. OCR specified that for recruitment purposes, the exception could only be used by individuals considered to be members of the covered entity's workforce.[28] Using or disclosing PHI for recruitment by a non-workforce member must meet one of the other exceptions to be permitted by the Privacy Rule.

Research on decedents' Information[29]

A covered entity may use or disclose PHI of a decedent to the researcher, if the researcher provides: (1) a representation that the use or disclosure sought is solely for research on the PHI of decedents; (2) documentation, at the covered entity's request, of the death of the specified individuals; and (3) a representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

De-identified Data Sets

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual.A covered entity may use or disclose de-identified health information for any purpose without restriction (although other laws may apply). The Privacy Rule designates two ways by which a covered entity can determine that health information is de-identified.The first is the "Safe Harbor" approach, which permits a covered entity to consider data to be de-identified if it removes 18 types of identifiers (*e.g.*, names and other direct identifiers, such as medical record numbers or social security numbers, all elements of dates other than year, age if over 89, all geography smaller than a state, and all but the first three digits of zip codes unless the first three digits represent a population with less than 20,000 inhabitants (to which it must be replaced with 000, and some other identifiers). The covered entity must also have no actual knowledge that the remaining information could be used to identify an individual, either alone or in combination with other information. An alternative is the statistical approach, which permits covered entities to disclose health information in any form provided that a qualified statistical or scientific expert concludes, through the use of accepted analytic techniques, that the risk the information could be used alone, or in combination with other reasonably available information, to identify the subject is very small.

The Privacy Rule permits covered entities to develop procedures under which a statistician or similarly qualified person may determine that the risk of re-identification of the information in a given data set is very small.[30]

Section 13424(c) of the HITECH Act requires the secretary of HHS to issue guidance on how best to implement the requirements for the de-identification of health information contained in the Privacy Rule.

In the Omnibus Rule, HHS notes that "we decline to completely exempt limited data sets from these provisions as, unlike de-identified data, they are still protected health information. However, disclosures of limited data sets for purposes permitted under the Rule would be exempt from the authorization requirements to the extent the only remuneration received in exchange for the data is a reasonable, cost-based fee to prepare and transmit the data or a fee otherwise expressly permitted by other law."[31]

The Privacy Rule, modified by the Omnibus Rule, includes a new Section 164.532(f). This section indicates "that a covered entity may continue to use or disclose a limited data set in accordance with an existing data use agreement that meets the requirements of Section 164.514(e), including for research purposes, until "the data use agreement is renewed or modified or until one year from the compliance date of this final rule [September 23, 2013], whichever is earlier, even if such disclosure would otherwise constitute a sale of protected health information upon the effective date of this rule."[32]

Limited Data Sets[33]

Soon after the final Privacy Rule was released in 2000, many researchers found that the restrictions imposed by its de-identification standards were impractical and would force researchers to seek waivers for research that otherwise was exempt from IRB review.[34]

In amendments to the regulation released in August 2002, the HHS created an alternative mechanism to use or disclose data for research, dubbed a "limited data set." Unlike a de-identified data set, a limited data set may include geographic information other than street address, all elements of dates and ages, and certain other unique identifying characteristics or codes.

For information to be shared in a limited data set, the recipient must agree to sign a Data Use Agreement (DUA).

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

The use of a DUA assures the covered entity that the recipient will, among other things, protect the limited data set and not make any effort to re-identify individuals using the data set or contact individuals if re-identified.A researcher may be a business associate if the researcher performs a function, activity, or service for a covered entity that does fall within the definition of business associate, such as the healthcare operations function of creating a de-identified or limited data set for the covered entity. Where the researcher is also the intended recipient of the de-identified data or limited data set, the researcher must return or destroy the identifiers at the time the business associate relationship to create the data set terminates and the researcher may then wish to use the de-identified data or limited data set (subject to a DUA) for research purpose.

In the Omnibus Rule, the HHS encourages covered entities and business associates to take advantage of the safe harbor provision of the breach notification rule by encrypting limited data sets and other protected health information pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 Fed. Reg. 42740, 42742). "If protected health information is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information."[35]

3. Additional Protections and Mandates

To protect against inappropriate use or disclosure of PHI, the Privacy Rule imposes numerous detailed administrative requirements on covered entities, many of which affect research. These include a "minimum necessary" standard applicable to many research-related uses and disclosures of PHI, as well as a requirement that covered entities contracting with third parties to perform treatment, payment, or healthcare operations activities (note, this list intentionally does not include research) on their behalf must enter into "business associate agreements" with those third parties.

Minimum Necessary Standard

HIPAA requires covered entities to make reasonable efforts to limit the PHI used, disclosed, or requested for any purpose other than direct treatment to the "minimum necessary" to accomplish the intended purpose of the use, disclosure, or request.[36] Although the principle addressed by the standard is laudable, its application is sometimes overly restrictive and may hamper appropriate research activities. It is, therefore, important for covered entities and researchers alike to understand the circumstances where the minimum necessary standard does not apply. These include:

- Disclosures to or requests by a healthcare provider for treatment (which may include research-related treatment)
- Uses or disclosures made pursuant to a written authorization
- Uses or disclosures required by law, including uses or disclosures made to public health authorities such as the Public Health Service's Office for Human Research Protections (OHRP) or the Food and Drug Administration (FDA); and uses or disclosures made to FDA-regulated entities that in turn are required to make safety, efficacy, or quality reports to FDA related to drugs, devices, or biologics that they manufacture.

Business Associate Agreements

The HIPAA statute's administrative simplification and privacy standards apply only to covered entities. To address concerns that the legislation left unregulated scores of individuals and organizations—ranging from

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

software vendors to disease management companies to accreditation agencies—with broad access to PHI, the HHS imposed on covered entities an obligation to enter into specific written agreements (called "business associate agreements" or BAAs) with these third parties that, in effect, extended the Privacy Rule (and, later the Security Rule) to a much broader segment of the healthcare industry.

The Omnibus Rule clarified the role of researchers and business associates. The rule includes a new definition of a business associate as an entity that "creates, receives, maintains or transmits PHI"[37] for a function or activity regulated by HIPAA, on behalf of a covered entity.

An external researcher is not a business associate of a covered entity by virtue of its research activities, even if the covered entity has hired the researcher to perform the research thus other HIPAA compliant methods must be utilized other than Business Associate Agreements for a covered entity to disclose identifiable PHI to a researcher.[38] Similarly, an external or independent IRB is not a business associate of a covered entity by virtue of its performing research review, approval, and continuing oversight functions. However, a researcher may be a business associate if the researcher performs a function, activity, or service for a covered entity that does fall within the definition of business associate, such as the healthcare operations function of creating a de-identified or limited data set for the covered entity.

Common Rule and FDA Privacy and Confidentiality Provisions

The Common Rule defines "private information" to include "information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record)."[39] One can argue that, since implementation of the Privacy Rule, private information includes (though may not be limited to) any information that constitutes PHI under HIPAA.

Ethical guidelines that influenced the adoption and content of the Common Rule and corresponding FDA regulations stress the importance of participant privacy and the need to protect the confidentiality of research data. The regulations include standards requiring researchers to inform participants of their privacy rights and requiring IRBs to assure research plans include adequate provisions to protect the privacy of subjects and maintain the confidentiality of data.[40] The distinction between these two terms is not conceptually obvious to many, but understanding it can help IRBs and researchers to assure that both sets of interests are well protected. In general, privacy "refers to persons; and to their interest in controlling the access of others to themselves." Confidentiality, by contrast, "refers to data; and to the agreements that are made about ways in which information is restricted to certain people."[41]

1. Participant Privacy and Informed Consent

Research participant privacy interests are addressed primarily through the informed consent process. The Common Rule and corresponding FDA regulations require the consent to include information about the study and the subject's participation in the study, as well as a "statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained." FDA regulations also require explicit discussion of the possibility that FDA may inspect research records.[42] Collectively, these requirements assure that prospective subjects can make an informed choice about whether they are willing to accept some intrusion as a condition of participating in a study.

It is difficult to protect subjects before they are contacted. Accordingly, researchers must understand that

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

prospective subjects and their families are at risk of harm particularly during the identification and recruitment phases of a study, before they are provided an opportunity to agree or decline to participate. For example, subjects may not be aware of their condition before they are contacted; or the process of contacting them may result in disclosures to family or household members who are unaware of their condition.[43] A researcher can minimize these risks in a number of ways, including approaching a prospective participant through his or her physician and using any predetermined methods and/or limitations of such contact.

2. Confidentiality Protections

It is often the case in data research that there is enough –built-in "privacy/confidentiality by design" protections that the research activity is exempt from further oversight of an IRB. This exempt classification is reserved for when the researchers do not use any identifiers for the research, in essence making the research de-identified. In research that does not include interaction or intervention with the subjects and only involves use of their de-identified data that was or (under the revised Common Rule) would have been gathered absent the research, such an –IRB-exempt determination can be made by the institution.

For non-exempt research, confidentiality concerns are reviewed and addressed primarily through the IRB's evaluation of the non-exempt research protocol and, in particular, its provisions for securing research data against inappropriate use and disclosure. These might include any combination of physical safeguards (*e.g.*, maintaining data in locked file cabinets in secure buildings or offices); electronic safeguards (*e.g.*, encrypting data and storage devices); and policy safeguards (*e.g.*, limiting data access to those with a documented need-to-know, training those with access to comply with approved security procedures, coding data and maintaining links in separate paper files or separate computers or servers, and destroying links at the earliest possible opportunity).

Researchers may also take advantage of available legal safeguards. For example, the National Institutes of Health (NIH), issues certificates of confidentiality(COCs) to protect research data against involuntary disclosure. COCs are available for both federally and non-federally supported research, and exempt a researcher from compliance with subpoenas, court orders, and even demands from law enforcement authorities, although they do not exempt researchers from mandatory public health disclosures such as communicable disease or abuse/neglect reports to state authorities.[44] The 21st Century Cures Act (passed in December 2016) made COC coverage automatic for affected federally funded research (thus eliminating the need to actually apply for one), while also supporting that non-federally funded research could still obtain one through application.

3. Secondary Use

The secondary use of one's personal data is hotly debated in contemporary times. While most of the press focuses on items such as social media and retail/service giants using one's data for purposes not disclosed or permissioned, the importance is not lost on the secondary use of research data. Under today's standards, unless otherwise committed to with the participant, information provided for one purpose can be de-identified and used for secondary purposes as de-identified data is not regulated by HIPAA or the Common Rule. This introduces many ethical questions on the appropriateness of secondary use of one's data in a manner that is not inconsistent with the original consent. While regulatory compliance can be met (through de-identification), such use may be inconsistent with the original intent (whether implied or written). One of the most famous examples of this was the secondary use of data and biospecimens from the Havasupai Tribe, where Arizona State University researchers were accused of using the data in manners inconsistent with the original informed consent.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

This issue is becoming more complicated as just as there are efforts to secure privacy and confidentiality of one's data, there is growing interest in making research data more transparent. Many institutions that conduct large amounts of NIH-funded studies have been familiar with data transparency requirements for many years (*i.e.*, data bought using taxpayer dollars belongs to the taxpayers, assuming privacy and confidentiality of the individuals to which the data is about is maintained)[45]. Similarly, many nonprofit foundations (such as the Wellcome Foundation or the Bill & Melinda Gates Foundation) that fund research also require that the de-identified data generated from their funding be made available to future researchers. In addition to sponsors of research making these demands for data sharing, a growing number of influential external entities are also making similar demands. Clinical (de-identified) data transparency is now required under Policy 0070 for approval filings with the European Medicines Agency and Canada is drafting a similar policy. Although FDA has yet to initiate such a requirement for filings in the United States, research data is often gathered and used for international filings thus a site in the United States could have their de-identified data made available to the public when filed in these other countries. In July 2018, the International Committee of Medical Journal Editors (ICMJE), whose members are editors of more than 4,000 medical journals, passed their requirement that requests to publish clinical trials in their member journals must be accompanied with a (de-identified) data sharing plan,and the requirement expands to require a data sharing plan posting on the trial's public registration beginning January 2019. Technically the submitted data sharing plan can be that the researchers will not share the data, however, it is expected that the journals will react negatively to the requirement in their consideration to publish or not publish the results of clinical trials in their journals.

In the revised Common Rule, a new element of consent requires that researchers disclose up front if they will or will not intend to use the data gathered for secondary research. Specifically, the new regulation requires the following in the consent form:

> "One of the following statements about any research that involves the collection of identifiable private information or identifiable biospecimens:
>
> (i) A statement that identifiers might be removed from the identifiable private information or identifiable biospecimens and that, after such removal, the information or biospecimens could be used for future research studies or distributed to another investigator for future research studies without additional informed consent from the subject or the legally authorized representative, if this might be a possibility; or
>
> (ii) A statement that the subject's information or biospecimens collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies."[46]

Given just the above demands for data transparency much less the growing ones from other stakeholders, it would be extremely impractical for a researcher to commit to option (ii) above. If a researcher wants to make such a commitment, the researchers should assure they have complete control over the data (including data that any subcontractors or vendors may have) and its destruction.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.