Published in final edited form as:

Clin Trials. 2015 October ; 12(5): 520–529. doi:10.1177/1740774515597677.

Privacy and confidentiality in pragmatic clinical trials

Deven McGraw¹, Sarah M. Greene², Caroline S. Miner³, Karen L. Staman⁴, Mary Jane Welch⁵, and Alan Rubel⁶

¹Manatt, Phelps & Phillips, LLP, Washington D.C., USA

²Patient-Centered Outcomes Research Institute, Washington, D.C., US

³Kaiser Permanente, NW Region, Portland, OR, USA

⁴CHB Wordsmith, Inc, Raleigh, NC, USA

⁵Rush University Medical Center, Chicago, IL, USA

⁶University of Wisconsin, Madison, WI, USA

Abstract

With pragmatic clinical trials (PCTs) an opportunity exists to answer important questions about the relative risks, burdens, and benefits of therapeutic interventions. However, concerns about protecting the privacy of this information are significant and must be balanced with the imperative to learn from the data gathered in routine clinical practice. Traditional privacy protections for research uses of identifiable information rely disproportionately on informed consent or authorizations, based on a presumption that this is necessary to fulfill ethical principles of respect for persons. But frequently the ideal of informed consent is not realized in its implementation. Moreover, the principle of respect for persons,—which encompasses their interests in health information privacy,—can be honored through other mechanisms. Data anonymization also plays a role in protecting privacy but is not suitable for all research, particularly PCTs. In this paper we explore both the ethical foundation and regulatory framework intended to protect privacy in PCTs. We then review examples of novel approaches to respecting persons in research that may have the added benefit of honoring patient privacy considerations.

Keywords

Privacy; Pragmatic Clinical Trials; Autonomy; Respect for Persons; Fair Information Practice Principles (FIPPs)

Address for Correspondence: Alan Rubel, University of Wisconsin-Madison, 4259 H.C. White Hall, 600 N. Park St., Madison, WI 53706.

Declaration of Conflicting Interests

Deven McGraw is the head of the PCORnet Data Privacy Task Force and has no other potential conflicts of interest to report. Sarah M Greene, Caroline Miner, Karen L Staman, Mary Jane Welch, and Alan Rubel have no conflicts of interest.

Introduction

Much of standard clinical practice is not informed by high-quality evidence,¹ and health information could be leveraged to improve the knowledge base and inform the care of individuals around the globe.² If correctly designed, pragmatic clinical trials (PCTs) will be uniquely capable of harnessing the proliferation of health information gathered at the point of care to investigate questions regarding comparative balance of benefits, burdens, and risks of biomedical or behavioral health interventions at the individual or population level. However, patients have consistently expressed concerns about the privacy and confidentiality of their health information, and these concerns are made particularly salient by the explosion in the collection of personal data in other domains, and growing concerns about the extent to which these data are accessed to meet a range of purposes.³ Recent, well-publicized breaches by health insurers Anthem (80 million records) and Premera (affecting 11 million individuals) are likely to deepen these concerns.^{4,5}

Traditionally, policies to protect privacy in research have relied on anonymization of the data and, in the case of research using identifiable information, seeking the prior consent or authorization of the individual. But there is a large gap between the ideal of informed consent and the practice of obtaining consent or authorization in practice.^{6,7} Consent forms are often too lengthy or opaque for people to understand,⁸ people are unlikely to read the forms in any case,⁹ and people may not have (or feel they have) a reasonable alternative to consenting. Data anonymization is useful for protecting privacy but is neither infallible nor suitable for all research.

We must balance the need to improve the evidence base through PCTs and protect privacy: both are important and one should not be compromised for the sake of the other. Protecting the privacy of individuals while still allowing health data to be leveraged for the common good requires a re-examination of our ethical framework and innovative approaches for protecting autonomy and privacy in sharing information in the context of PCTs.

In this paper we explore both the ethical foundation and regulatory framework that influence the use of data in PCTs. We then review examples of novel approaches to informed consent and authorization that are deployed primarily to address concerns about ethical treatment of research subjects and may have the added benefit of addressing privacy considerations while advancing research.

Privacy's Ethical Foundation

Defining privacy

There is no single, universally accepted definition of privacy. One prominent view of privacy is the ability to control the collection, use, and disclosure of one's personal information.¹⁰ While control over one's information may be morally important, it is not clear that privacy is best *defined* in terms of control. Privacy is elsewhere defined in terms of whether others can access one's information, regardless of whether it is the individual who is in control of her information,^{11,12} or whether information flows violate contextual

norms.¹³ Some recent accounts understand privacy in terms of whether others know or can make reasonable inferences about a person.^{14,15}

Respect for persons

Because health information is associated with some of our deepest, most personal, and most intimate facets, privacy in health information is a component of the principle of respect for persons. This principle is grounded in the idea of autonomy: that individuals are capable of self-governance and making important decisions about their lives for themselves and according to their values.^{16–18}

Respect for persons demands that sharing health information occur only under appropriate conditions, to appropriate parties, and for appropriate reasons. And it requires affording persons ample opportunity to protect their privacy.¹⁹ Further, when people seek health care they place trust in their care providers, insurers, and anyone using their health information.^{20,21} That trust is based on an implicit expectation that they will be treated with respect, including the expectation that their health information will not be used or disclosed inappropriately. Failure to live up to such a reasonable expectation violates that trust and undercuts individuals' autonomy interests.

Optimal Care

Health information privacy also helps ensure that people receive optimal care.²² When people are concerned about their health information privacy, they may engage in “privacy-protecting behaviors” such as avoiding healthcare altogether, lying to their care providers about their conditions, or seeking care out of their area.^{23,24} For example, according to a study published in 2013, nearly one in eight patients have withheld information from a healthcare provider because of privacy and security concerns.²²

Harms

Information disclosure can have direct negative effects on individuals' well-being and may lead to harms. Harm can happen when health information is misused, undermining a person's ability to secure employment, get insurance, or hold positions of responsibility, which limits autonomy. These opportunities help people to participate fully in society and are crucial for respect for persons.²⁵ Moreover, privacy in health information may help individuals avoid social stigma associated with certain health conditions. Such harms may conflict with *non-maleficence*, or the principle that one should do no harm to patients or communities. Harms can derive from information being misused (e.g., disclosure of research information to non-researchers or use of that information for non-research purposes) or from being used—even by researchers—in ways that are disagreeable to data subjects.

Justice

How individuals' health information is used also invokes questions of justice. For example, de-identified data may be used to discern racial or ethnic disparities in health issues, but also could create stigmas or harden stereotypes along racial and ethnic lines, even where no particular person is identified.^{26,27} Such stigmas and stereotypes are substantial barriers to participation in a modern, pluralistic society. And because stigmas and stereotypes are

unjustifiable grounds for the distribution of important social goods, such barriers create an injustice. Such issues can arise even when information is used as part of research intended to create generalizable knowledge.

Fair Information Practices

As noted above, privacy legal frameworks frequently rely on consent to uses and disclosures to protect autonomy. But respect for persons and protection of autonomy is also supported by other information practices. For example, fair information practice principles (FIPPS) promote data stewardship, provide a foundation for privacy laws in the U.S. and abroad, demonstrate respect for persons, and protect autonomy.²⁸ The core components of FIPPS in one widely used framework, along with connections of those components to ethical principles, are shown in Table 1. Providing individuals with choices regarding uses and disclosures of their information is just one of the FIPPs and is not absolute. Instead, the FIPPs collectively obligate persons and entities who collect, access and disclose information to adopt responsible data stewardship practices, regardless of whether or not the data subjects have provided consent. Such an approach assures that the “burden” for protecting data privacy rests primarily on the data holders.

What patients want

Proponents of reliance on consent to honor autonomy and respect for persons have looked to survey research to reinforce their views. For example, in a survey of 217 patients from four Veteran Affairs facilities, all of them were willing to share their medical records but recommended that procedures be instituted to give them control over whether and how their medical records are used for research.³¹

But the outcome of survey data may depend on how the questions are asked and whether the research is done with other protections for privacy, such as removal of identifiers. If the data are de-identified, 86% of respondents in one study said they were willing to have their data used for research, but only 35% were willing to share their data in a database that included identifiable information.³² Public views on this issue also may be evolving. A 2014 survey conducted by Truven Health and National Public Radio suggests that with the increased use of electronic medical records by physicians and hospitals, patients are getting more comfortable with collection and sharing of digital health data, including for research purposes. Two-thirds of respondents expressed willingness to share their health information for research purposes, as long as it was scrubbed of identifying details.³³ Yet another article suggests that patients place as much importance on the purpose for obtaining their information (research versus marketing) as whether consent is obtained.³⁴

Although survey data is an insufficient basis for establishing or changing research policies, the data potentially indicate an increasing level of comfort with research uses of health information, assuming steps are taken to protect an individual’s identity. Hence, models for protecting privacy in research that rely less on prior consent to each and every research protocol and more on other, FIPPs-based mechanisms for honoring individual’s privacy interests may be increasingly consistent with public opinion.

Current Regulatory Framework in the United States

Currently, data generated by PCTs come from clinical records of health care providers, administrative claims records of health plans, and, increasingly, from the patient directly, such as through patient-reported outcomes. In the U.S, research uses of information captured in clinical or claims records are likely to be governed by the Health Insurance Portability and Accountability Act regulations (HIPAA),³⁵ and by the Common Rule,³⁶ which governs the ethical conduct of human subjects research in circumstances where the research is federally supported or being conducted by an institution or organization that has agreed, in a federal-wide assurance agreement, to be bound by federal research rules. There are other federal rules, such as those issued by the Food and Drug Administration (FDA), providing protections for certain types of research or for other types of personal information that may be used in research.^{37–40} States may also regulate research uses of personal information. In the interest of brevity, this paper focuses exclusively on how HIPAA and the Common Rule govern research uses of personal information. Of note, information generated from data sources not covered by HIPAA (for example, data generated by consumers on social networking sites or in mobile apps) may not be covered by any privacy laws, depending on who is collecting the data.

Both HIPAA and the Common Rule rely significantly on the consent or express authorization of the individual before identifiable information can be used for “research” purposes (Table 2). Both rules apply even in circumstances where the research presents no interventional risk, such as in retrospective or observational studies. HIPAA and the Common Rule provide for some exceptions to this requirement, for example, HIPAA authorization is not required for research on decedent’s data and limited activities “preparing” for research (such as developing research questions or determining the possibility of recruiting subjects).

Ordinarily, consent or authorization must meet certain criteria (Table 2) and must be provided in advance of research access to the data. However, both HIPAA and the Common Rule allow an Institutional Review Board (or a Privacy Board, in the case of HIPAA) to waive or modify this requirement (Table 3). Waiver authority allows an IRB to dispense with the requirement altogether; alteration authority allows IRBs to consider other mechanisms for gleaning an individual’s agreement or level of comfort with the research without obtaining a signed authorization or consent (e.g., oral agreement).⁴¹

HIPAA also requires research uses of identifiable health information to be conducted using the “minimum necessary” amount of information needed to address the research question.⁴¹ This provision is intended to assure that uses of health data are as minimally intrusive as possible on privacy. However, this requirement does not apply to research that has been authorized by the data subject,⁴¹ demonstrating the strong role authorization plays in brokering research uses of data. Entities covered by HIPAA also must adopt specific security protections for electronic identifiable health information;⁴¹ the Common Rule is silent with respect to data security.

Research Regulated More Stringently Than Other Uses of Health Data

Both HIPAA and the Common Rule recognize the need to protect the privacy of individual's information when used for research purposes, and both use the same definition for research: "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."^{36,41} But other uses of identifiable health information that may effect privacy interests are regulated far less stringently. The Common Rule regulates only uses of identifiable information for research purposes, so other activities—even when conducted by entities subject to the Common Rule—are not governed by its provisions. Under HIPAA, entities covered by the law are permitted to use information, without first needing to obtain the individual's authorization, in order to treat patients, to facilitate payment for care, and for a list of "health care operations (Table 4)." For example, a hospital can re-use clinical data to conduct quality assessment and improvement, including evaluating outcomes and developing clinical guidelines, "provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities." This creates perverse incentives: undertake quality improvement studies only in circumstances where the results are intended to be used internally, because intent to share knowledge triggers the definition of research and more comprehensive research requirements (including potentially triggering Common Rule coverage, if the entity conducting the study is covered by the Common Rule). Similarly, a topic or issue that could benefit from systematic investigation and an intent to share results may be handled as a quality improvement project to avoid the increased regulatory burden placed on research. Further, because the penalties for violating HIPAA include significant fines and the possibility of criminal prosecution, entities covered by HIPAA tend to interpret the regulations in a conservative way.⁴² Conservative approaches also may lead some IRBs and Privacy Boards to be reluctant to waive or modify consent or authorization requirements.³⁰

In material published with the final HIPAA research regulations, regulators note that the original proposal would have allowed entities covered by HIPAA to use or disclose without requiring prior individual authorization "knowledge related to health that can be applied to populations outside of the population served by the covered entity."⁴³ In other words, regulators believed that research designed to improve health care practices should have been included in the definition of health care operations. They do not provide an explanation for why this changed in the final rule; however, the discussion suggests that the health care industry and the regulators believed they were reducing administrative burden by harmonizing the research oversight under the Privacy Rule with the existing Common Rule. Although harmonization of regulatory regimes is desirable, the Common Rule's focus on protecting the ethical interests of human subjects may be a poor fit for governing re-use of data collected in clinical and administrative claims records.³⁰ In contrast, HIPAA focuses on data management and is only tangentially concerned with the type of interactions generating the data.

Anonymized (or De-Identified) Data

Neither HIPAA nor the Common Rule require prior consent or authorization if the information used in research is not identifiable, or where there is sufficiently low risk of

identifying an individual in a dataset. As noted above, the Common Rule regulates only research on human subjects, which is defined to include research using identifiable data. Data that have been “de-identified” in accordance with HIPAA standards are no longer covered by HIPAA regulations.⁴⁴ HIPAA also allows entities to use a “limited data set” for research purposes; such data has certain identifiers (such as name and address) removed or masked. Recipients must agree to a data use agreement setting forth the purposes for which the data can be used and prohibiting re-identification.⁴¹ Given the reduced regulatory constraints of using de-identified data or a limited data set, there are incentives to use such data for research purposes, and reducing the risk of re-identification is an important mechanism for respecting research subjects. But the removal of identifiers reduces the utility of the data for some types of research,⁴⁵ and in PCTs where the research takes place in the context of providing clinical care, it is more likely that identifiable data will need to be collected. Further, concerns have been raised about whether de-identification under HIPAA is sufficiently protective of an individual’s identity to justify the “hands off” regulatory approach.²⁰

Issues with HIPAA and the Common Rule

HIPAA’s research rules have been subject to harsh criticism. A report from an Institute of Medicine Committee in 2009 concluded that the HIPAA Privacy Rule does not protect privacy as well as it should and impedes important health research.³⁰ The report noted that the Privacy Rule is not uniformly applicable to all health research, overstates the ability of informed consent to protect privacy, conflicts with other federal regulations (like the Common Rule), is interpreted differently across institutions, creates barriers to research, and leads to biased research samples.³⁰ The requirement of both a HIPAA authorization and informed consent under the Common Rule raises concerns about privacy, confusion about the forms, mistrust or fear of research,⁴⁶ and inhibits medical record and database research.⁴⁷

Regulators have taken steps to make the consent and authorization process easier to facilitate research uses of identifiable information. In January 2013, the Department of Health and Human Services issued the “Omnibus Rule,” which included HIPAA guidance to allow individuals to sign single (compound) authorizations for multiple research projects and to broadly consent to use of their data for “future research” without having to authorize such research study by study.⁴⁸

The Office for Human Research Protections (OHRP), which oversees the Common Rule, is considering whether it should lessen regulation of research re-uses of data collected initially as clinical or administrative data. In 2011, it issued an Advance Notice of Proposed Rulemaking (ANPRM), which issued for public comment potential changes to the Common Rule intended to harmonize it with HIPAA and to modernize, simplify and enhance it.⁴⁹ Of importance for some PCTs, OHRP proposed that research on data collected for clinical purposes but secondarily used for research purposes would be exempt from required IRB review; instead, researchers could file a one to two-page registration of the study with the IRB/institution. Written, informed consent would still be required for such research (when

using identifiable information), but it could be obtained at the time of initial collection of the data.⁴⁹

Mechanisms for Honoring Privacy Interests and Autonomy

A number of national initiatives, including the Patient-Centered Outcomes Research Institute's (PCORI) National Patient Centered Outcomes Research Network (PCORnet) and the National Institutes of Health (NIH) Health Systems Research Collaboratory (Collaboratory), are catalyzing new infrastructures for PCTs and are developing ways that respect and protect the autonomy and privacy of research participants yet go beyond reliance on traditional informed consent. Below, we explore examples of innovative approaches to respecting the autonomy and rights of individuals. In many of these examples, the different approaches to "consent" or more fully engaging individuals in research were implemented as part of an IRB assessment that the research posed minimal interventional risk. But the approaches, which leverage other aspects of the FIPPs such as "openness and transparency," also have the benefit of protecting privacy while advancing research. Currently there is no consensus on which approach works best for what types of research; consequently, approaches to protecting privacy that do not rely on opt-in consent should be investigated to create an evidentiary base for privacy frameworks for PCTs.

Greater input into research and research policies

PCORI was developed to improve the evidence base and help patients, caregivers, clinicians and other stakeholders make informed health-care decisions; it requires funded research to be patient-centered, which includes directly engaging people representing the study population of interest.⁵⁰ PCORI has supported the development of PCORnet, which is a federated network that includes 29 sites, 18 of which are patient-powered networks and 11 of which are clinical data research networks. Although each individual network determines its own approach to engaging individuals in research, a PCORnet Patient Council (PPC) acts as a patient advisory group to the PCORnet steering committee and leadership, which generates policies and best practices. Likewise, the Collaboratory Stakeholder Engagement Core includes patient and consumer representatives and serves as an advisory group, providing feedback to the Collaboratory leadership on study design and implementation issues and suggesting approaches for partnering with stakeholders.⁵¹

Opt out

By giving informed consent, participants "opt in" to a traditional research trial. However, in an "opt out" model, participants are included automatically, but can either opt out completely or allow selected data to be used (opt out with restrictions).⁵² The Collaboratory study, Strategies and Opportunities to Stop Colorectal Cancer in Priority Populations (STOP CRC),⁵³ uses an opt out mechanism for participants. Briefly, in an effort to improve rates of colorectal-cancer screening among the predominantly minority and low-income patients who receive health care services through Federally Qualified Health Centers (FQHCs), a fecal immunochemical test (FIT) kit is mailed to patients aged 50–74 who were not up-to-date with colorectal-cancer screening guidelines. These participants were identified through the electronic medical record, and an information letter was sent prior to mailing the FIT

with the option to opt out.⁵⁴ Participants are reminded by post card or phone to complete their tests. The participant may choose to opt out by contacting the FQHC; those who do not return the kit will receive additional reminders (unless they opt-out).

Broad Notification

In minimal risk studies, broad notification through posters, emails, brochures, social media or web portals may be sufficient to protect autonomy. For example, the Randomized Evaluation of Decolonization versus Universal Clearance to Eliminate MRSA (REDUCE MRSA) trial,³⁰ compared three strategies in current use for preventing methicillin-resistant *Staphylococcus aureus* (MRSA) infections in adult intensive care units (ICUs) of a single health system. In this case, a waiver of informed consent was granted, although the IRB required that patients be informed of the study through notices posted in each ICU room. This approach does not seek consent but respects participants by providing information about the new bathing procedure and the rationale for why it is being done.

Individual Notification

Individual notification increases transparency and helps ensure that patients are adequately informed about the research in which they are participating and may include opt out information. Even when a waiver of consent is granted, informing and notifying patients is a way of respecting their interests, and offering a mechanism for opting out helps preserve their autonomy. For example, the Collaboratory's Time to Reduce End Stage Renal disease (TiME) trial is a cluster-randomized trial that evaluates a minimum hemodialysis session duration of at least 4.25 hours (if determined medically appropriate by the treating nephrologist) compared with usual care (no trial-driven approach to session duration) for patients with end-stage renal disease to improve survival and quality of life for patients with kidney failure.⁵⁵ All patients initiating treatment with maintenance hemodialysis at participating facilities are provided with written information that includes the trial sponsor, the purpose of the trial, the treating physician's role, a description of the transmission of de-identified patient data to the University of Pennsylvania, a statement that no additional testing will be performed for the trial, and a toll-free telephone number to contact with questions or to opt-out of participation.

Community Consultation

Another approach to respecting individuals in research without relying on individual consent is community consultation, in which people agree to be governed by the decisions of community representatives with respect to research uses.⁶ This method turns the focus away from individual control and choice to agreement on a governance framework,⁶ and was deployed by the Secretary's Advisory Committee on Genetic Testing when the genome was being mapped to help determine the risks and disclosures needed for genetic testing.

Conclusions

Reaping the full benefits from the nation's investment in digitizing health data and research will require balancing—not trading off—the need to protect the privacy of individuals while allowing health data to be leveraged for the common good. Honoring individuals' privacy

interests and autonomy is at the heart of the social compact between study participants and researchers. Current privacy law, based in part on the responsible data stewardship principles of Fair Information Practices, provides some boundaries and safeguards for re-use of health data for research purposes. However, the laws are not tailored to address the privacy risks that arise with research uses of data, and may provide some disincentives to re-use of data. In addition, research rules designed to protect human subjects against interventional risks may not be the best mechanisms for addressing risks to privacy. The modified approaches to “consent” and engagement deployed in projects with minimal risk interventions may ultimately prove effective at honoring individual’s privacy interests in data—but the impact of these novel approaches on privacy has not been explored. Creating a trusted, robust ecosystem for PCTs requires further study regarding what protections are effective at addressing privacy concerns and, over the longer term, regulatory reform to assure that the “protections” deployed in the name of privacy effectively address the risks.

Acknowledgments

Robert Califf and Jeremy Sugarman provided input on earlier versions of this manuscript. The authors thank Tammy Reece for help with putting the manuscript together. The views presented here are solely the responsibility of the authors and do not necessarily represent the official views of the National Institutes of Health or of the Patient-Centered Outcomes Research Institute (PCORI), its Board of Governors or Methodology Committee, or other participants in the National Patient-Centered Clinical Research Network (PCORnet).

Funding

This work was supported by the National Institutes of Health (NIH) Common Fund, through a cooperative agreement (U54 AT007748) from the Office of Strategic Coordination within the Office of the NIH Director. Additional support was provided by the Patient-Centered Outcomes Research Institute (PCORI) Award for development of the National Patient-Centered Clinical Research Network (PCORnet).

References

1. Tricoci P, Allen JM, Kramer JM, et al. Scientific evidence underlying the ACC/AHA clinical practice guidelines. *JAMA*. 2009; 301:831–841. [PubMed: 19244190]
2. Committee on the Learning Health Care System in America, Institute of Medicine. *Best Care at Lower Cost: The Path to Continuously Learning Health Care in America*. Washington (DC): National Academies Press (US); 2013. <http://www.ncbi.nlm.nih.gov/books/NBK207225/> accessed 28 January 2015
3. Executive Office of the President. *Big Data: Seizing Opportunities, Preserving Values*. 2014. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf accessed 20 January 2014
4. Rathburn, J.; Hennessy, J.; Barlament, J. Another Day Another Cyberattack: Premera Blue Cross Announces Large Data Breach. *Safe & Sound: A Privacy and Security Blog from Quarles & Brady*. 2015. <http://safeandsound.quarles.com/2015/03/another-day-another-cyberattack-premera-blue-cross-announces-large-data-breach/>
5. Barlament, J.; Rathburn, J. Were you affected by the Anthem breach? Answers to these questions may help. *Safe & Sound: A Privacy and Security Blog from Quarles & Brady*. 2015. <http://safeandsound.quarles.com/2015/02/were-you-affected-by-the-anthem-breach-answers-to-these-questions-may-help/>
6. Koenig BA. Have we asked too much of consent? *Hastings Cent Rep*. 2014; 44:33–34. [PubMed: 25043364]
7. Henderson GE. Is informed consent broken? *Am J Med Sci*. 2011; 342:267–272. [PubMed: 21817873]

8. Paasche-Orlow MK, Taylor HA, Brancati FL. Readability standards for informed-consent forms as compared with actual readability. *N Engl J Med*. 2003; 348:721–726. [PubMed: 12594317]
9. McGraw D, Dempsey JX, Harris L, et al. Privacy as an enabler, not an impediment: building trust into health information exchange. *Health Aff (Millwood)*. 2009; 28:416–427. [PubMed: 19275998]
10. Westin, AF. Privacy and freedom. London: Bodley Head; 1970.
11. Allen, AL. Uneasy access: privacy for women in a free society. Totowa, N.J: Rowman & Littlefield; 1988.
12. Presidential Commission for the Study of Bioethical Issues. Privacy and Progress in Whole Genome Sequencing. 2012. <http://bioethics.gov/sites/default/files/PrivacyProgress508.pdf> accessed 15 January 2015
13. Nissenbaum, HF. Privacy in context: technology, policy, and the integrity of social life. Stanford, Calif: Stanford Law Books; 2010.
14. Rubel A. The Particularized Judgment Account of Privacy. *Res Publica*. 2011; 17:275–290.
15. Blaauw M. The Epistemic Account of Privacy. *Episteme*. 2013; 10:167–177.
16. Beauchamp, TL. Principles of biomedical ethics. 7th. New York: Oxford University Press; 2013.
17. The Belmont Report | HHS.gov. <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html> (accessed 9 June 2014)
18. Brock DW. A critique of three objections to physician-assisted suicide. *Ethics*. 1999; 109:519–547. [PubMed: 11657610]
19. Stanley, IB. Benn, 'Privacy, Freedom, and Respect for Persons', in Privacy: Nomos XIII. Pennock, J.; Chapman, J., editors. New York: Atherton Press; 1971.
20. Rothstein MA. Is deidentification sufficient to protect health privacy in research? *Am J Bioeth*. 2010; 10:3–11. [PubMed: 20818545]
21. Hall MA, Dugan E, Zheng B, et al. Trust in physicians and medical institutions: what is it, can it be measured, and does it matter? *Milbank Q*. 2001; 79:613–639. v. [PubMed: 11789119]
22. Agaku IT, Adisa AO, Ayo-Yusuf OA, et al. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J Am Med Inform Assoc*. 2014; 21:374–378. [PubMed: 23975624]
23. California Healthcare Foundation. Consumers and Health Information Technology: A National Survey. 2010. <http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey>
24. Goldman J. Protecting privacy to improve health care. *Health Aff (Millwood)*. 1998; 17:47–60. [PubMed: 9916354]
25. Rubel, A. Autonomy, Surveillance, and Privacy in The Routledge Companion to Bioethics. Arras, John; Kukla, Rebecca; Fenton, Elizabeth, editors. 2014.
26. Francis LP, Francis JG. Group Compromise: Perfect Cases Make Problematic Generalizations. *The American Journal of Bioethics*. 2010; 10:25–27. [PubMed: 20818553]
27. Hausman DM. Group risks, risks to groups, and group engagement in genetics research. *Kennedy Inst Ethics J*. 2007; 17:351–369. [PubMed: 18363270]
28. U.S. Department of Health, Education & Welfare. Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 1973. <http://www.justice.gov/opcl/docs/rec-com-rights.pdf> accessed 15 January 2015
29. Markle Foundation. The Markle Connecting for Health Common Framework for Networked Personal Health Information. 2008. <http://www.markle.org/health/markle-common-framework/connecting-consumers/overview> accessed 15 January 2015
30. Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington (DC): National Academies Press (US); 2009. <http://www.ncbi.nlm.nih.gov/books/NBK9578/> accessed 15 December 2013
31. Damschroder LJ, Pritts JL, Neblo MA, et al. Patients, privacy and trust: patients' willingness to allow researchers to access their medical records. *Soc Sci Med*. 2007; 64:223–235. [PubMed: 17045717]

32. Kass NE, Natowicz MR, Hull SC, et al. The Use of Medical Records in Research: What Do Patients Want? *The Journal of Law, Medicine & Ethics*. 2003; 31:429–433.
33. Truven Health analytics, National Public Radio (NPR). Data Privacy Health Poll. 2014. http://truvenhealth.com/Portals/0/NPR-Truven-Health-Poll/NPRPulseDataPrivacy_Nov2014.pdf
34. Grande D, Mitra N, Shah A, et al. The importance of purpose: moving beyond consent in the societal use of personal health information. *Ann Intern Med*. 2014; 161:855–862. [PubMed: 25506854]
35. Department of Health and Human Services, Office for Civil Rights. Summary of the HIPAA Privacy Rule. 2003. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>
36. Code of Federal Regulations | HHS.gov. <http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html> (accessed 8 October 2014)
37. U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA). <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html> (accessed 16 January 2015)
38. Department of Health and Human Services. 46 CFR 42. Confidentiality of Alcohol and Drug Abuse Patient Records. <http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2> (accessed 26 January 2015)
39. National Institutes of Health. HIPAA Privacy Rule and Its Impacts on Research: How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?. 2007. http://privacyruleandresearch.nih.gov/pr_08.asp accessed 27 April 2015
40. U.S. Food and Drug Administration. FDA Regulations Relating to Good Clinical Practice and Clinical Trials. 2015. <http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/ucm155713.htm> accessed 16 June 2015
41. 104th Congress. Health Insurance Portability and Accountability Act of 1996. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf> (accessed 18 December 2013)
42. Armitage J, Souhami R, Friedman L, et al. The impact of privacy and confidentiality laws on the conduct of clinical trials. *Clin Trials*. 2008; 5:70–74. [PubMed: 18283083]
43. Department of Health and Human Services. Final Privacy Rule Preamble. Part 160 – subpart A – General Provisions. <http://aspe.hhs.gov/admsimp/final/PvcPre02.htm> (accessed 17 January 2015)
44. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html> (accessed 11 December 2014)
45. McGraw D. Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. *J Am Med Inform Assoc*. 2013; 20:29–34. [PubMed: 22735615]
46. Dunlop AL, Graham T, Leroy Z, et al. The impact of HIPAA authorization on willingness to participate in clinical research. *Ann Epidemiol*. 2007; 17:899–905. [PubMed: 17689261]
47. O'Herrin JK, Fost N, Kudsk KA. Health Insurance Portability Accountability Act (HIPAA) regulations: effect on medical record research. *Ann Surg*. 2004; 239:772–776. discussion 776–778. [PubMed: 15166956]
48. Goldstein MM, Pewen WF. The HIPAA Omnibus Rule: implications for public health policy and practice. *Public Health Rep*. 2013; 128:554–558. [PubMed: 24179268]
49. Department of Health and Human Services. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators. 2011
50. PCORI Methodology Committee. PCORI Methodology Standards. Dec 14. 2012 <http://www.pcori.org/assets/PCORI-Methodology-Standards1.pdf> accessed 8 October 2013
51. NIH Collaboratory. Stakeholder Engagement Webpage. <https://www.nihcollaboratory.org/cores/Pages/stakeholder-engagement.aspx> (accessed 28 April 2015)
52. Goldstein MM, Rein AR. Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis ERATIONS AND ANALYSIS. 2010

53. Coronado GD, Burdick T, Petrik A, et al. Using an Automated Data-driven, EHR-Embedded Program for Mailing FIT kits: Lessons from the STOP CRC Pilot Study. *J Gen Pract (Los Angel)*. 2014;2.
54. Coronado GD, Vollmer WM, Petrik A, et al. Strategies and Opportunities to STOP Colon Cancer in Priority Populations: design of a cluster-randomized pragmatic trial. *Contemp Clin Trials*. 2014; 38:344–349. [PubMed: 24937017]
55. Laura, Dember. Time to Reduce Mortality in End-Stage Renal Disease (TiME) A Large, Pragmatic Cluster Randomized Trial in Maintenance Hemodialysis. 2013

Table 1**Fair Information Practice Principles (FIPPS)**

Principle	Description (from The Markle Connecting for Health Common Framework for Networked Personal Health Information)²⁹	Link to Ethical Principles
Openness and Transparency	“Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.”	Openness and transparency allow individuals to better understand how their information is collected and used at all stages of the research process (including scientific publications), which is important for respecting persons independent of their choice in matters and, in some cases, targets the fundamental principle of the individual’s right to know.
Purpose Specification	“The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.”	Specifying purposes helps ensure that persons have the opportunity to understand and, in some cases, endorse the purposes to which their information is put, which is an important facet of respecting them as participants.
Collection limitation and data minimization	“Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.”	Because health information is associated with some of the deepest, most personal, and most intimate facets of ourselves, respect for persons demands that sharing health information occur only under appropriate conditions, to appropriate parties, and for appropriate reasons. Limiting collection and minimizing data helps ensure that sharing is limited to such circumstances.
Use Limitation	“Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.”	See comment under “collection limitation and data use.”
Individual Participation and Control	“Consumers should be able to control access to their personal information – specifically, they should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.”	Individual choice, or consent, is a component of the FIPPs, but it is not absolute, and the degree of choice may depend on how completely the other principles are exercised. Moreover, choice may be based on alternative models, such as opt out models that allow individuals with particularly acute privacy concerns to avoid information sharing, rather than seeking opt-in permission from all individuals. ³⁰
Data Quality and Integrity	“All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.”	Data integrity helps ensure that information attributed to people is actually about them, and hence that they are not treated unfairly or unjustifiably; again, this is important in respecting persons.
Security Safeguards and controls	“Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.”	Data security policies and technical requirements should be in place to help protect data and reinforce stewardship practices adopted to implement the other principles.
Accountability and Oversight	“Entities in control of personal health information must be held accountable for implementing these principles.”	Helps ensure entities controlling personal health information follow all of the principles.
Remedies	“Remedies must exist to address security breaches or privacy violations.”	Allowing persons to exercise control in effecting remedies is a crucial aspect of respecting persons whose data security or privacy has been breached.

Table 2

Privacy Requirements for consent under the Common Rule and authorization under HIPAA.

Common Rule (45 CFR 46.116) Consent ³⁶	HIPAA Authorization ³⁵ (45 CFR 164.508)
A statement that explains the purpose, duration, procedures, alternative procedures, risks and benefits of the research.	An authorization must be written in plain language with specific terms.
A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.	All authorizations must include information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.
A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.	Treatment, payment, enrollment, or benefits eligibility may not be a condition for authorization.

Table 3

Under the Common Rule and HIPAA, consent or authorization can be waived or altered if the following conditions are met:

Common Rule (45 CFR 46.116) ³⁶	HIPAA ⁴¹ (45 CFR 164.512(i))
The research involves no more than minimal risk to the subjects.	The use or disclosure of protected health information (PHI) involves no more than a minimal risk to the privacy of individuals (i.e., there is an adequate plan to protect identifiers, a plan to destroy the identifiers at earliest opportunity, and there are adequate assurances of no reuse or re-disclosure).
The research could not practicably be carried out without the waiver or alteration.	The research could not practicably be conducted without the waiver or alteration; and
The waiver or alteration will not adversely affect the rights and welfare of the subjects	The research could not practicably be conducted without access to and use of the protected health information.
Whenever appropriate, the subjects will be provided with additional pertinent information after participation	

Table 4

Health care operations include certain administrative, financial, legal, and quality improvement activities and are defined in 45 CFR 164.501 as follows:

Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination
Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities
Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims
Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs
Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity