3-31-2016

Privacy, Fairness, and Respect for Individuals

Dixie B. Baker
Martin, Blanck & Associates, Dixie.baker@martin-blanck.com

Jane Kaye
Oxford University, Jane.kaye@law.ox.ac.uk

Sharon F. Terry
Genetic Alliance, sterry@geneticalliance.org

The Electronic Data Methods (EDM) Forum is supported by the Agency for Healthcare Research and Quality (AHRQ), Grant 1U18HS022789-01. eGEMs publications do not reflect the official views of AHRQ or the United States Department of Health and Human Services.

Privacy, Fairness, and Respect for Individuals

Abstract

Introduction: Individuals have a moral claim to be involved in the governance of their personal data. Individuals' rights include privacy, autonomy, and the ability to choose for themselves how they want to manage risk, consistent with their own personal values and life situations. The Fair Information Practices principles (FIPPs) offer a framework for governance. Privacy-enhancing technology that complies with applicable law and FIPPs offers a dynamic governance tool for enabling the fair and open use of individual's personal data.

Perceptions of Risk: Any governance model must protect against the risks posed by data misuse. Individual perceptions of risks are a subjective function involving individuals' values toward self, family, and society, their perceptions of trust, and their cognitive decision-making skills.

The HIPAA Privacy Rule Puts Some Governance in the Hands of Individuals: Individual privacy protections and individuals' right to choose are codified in the HIPAA Privacy Rule, which attempts to strike a balance between the dual goals of information flow and privacy protection. The choices most commonly given individuals regarding the use of their health information are binary ("yes" or "no") and immutable. Recent federal recommendations and law recognize the need for granular, dynamic choices.

Building a Governance Framework Based in Trust: Avoiding Surprises: Individuals expect that they will govern the use of their own health and genomic data. Failure to build and maintain individuals' trust increases the likelihood that they will refuse to grant permission to access or use their data. The "no surprises principle" asserts that an individual's personal information should never be collected, used, transmitted, or disclosed in a way that would surprise the individual were she to learn about it.

Fair Information Practices Principles: The FIPPs provide a powerful framework for enabling data sharing and use, while maintaining trust. We introduce the eight FIPPs adopted by the Department of Health and Human Services, and provide examples of their interpretation and implementation.

Reducing Risk through Consumer Engagement: Privacy risk and health risk can be reduced by giving consumers control, autonomy, and transparency, and by engaging them in managing their own health. Explicit "consent" may not always be necessary – the FIPPs offer multiple ways to engender trust and avoid surprises. Platform for Engaging Everyone Responsibly (PEER) We describe the Platform for Engaging Everyone Responsibly (PEER), a technology solution that enables individuals to govern the access to and use of their health information, within an environment that espouses the FIPPs and "no surprises."

Conclusion: Fair and effective governance recognizes the individual's moral claim to maintain control over the contribution and use of their health and genomic information. Maintaining individuals' trust in an environment of transparency is essential to assuring continuing access to their data for safe and effective health care and biomedical knowledge advancement.

Acknowledgements

We acknowledge the work of Robert Shelton and Private Access. In addition, we also recognize the Genetic Alliance Staff and the Genetic Alliance Think Tank for their contributions.

Keywords
Participant governance, health information technology, patient involvement, privacy

Disciplines
Health Information Technology

eGEMs
Generating Evidence & Methods to improve patient outcomes

Governance Through Privacy, Fairness, and Respect for Individuals

Dixie B. Baker, PhD, MS, MS, FHIMSS;[i] Jane Kaye, DPhil, LLB, Grad. Dip. Leg.;[ii] Sharon F. Terry, MA[iii]

ABSTRACT

Introduction: Individuals have a moral claim to be involved in the governance of their personal data. Individuals' rights include privacy, autonomy, and the ability to choose for themselves how they want to manage risk, consistent with their own personal values and life situations. The Fair Information Practices principles (FIPPs) offer a framework for governance. Privacy-enhancing technology that complies with applicable law and FIPPs offers a dynamic governance tool for enabling the fair and open use of individual's personal data.

Perceptions of Risk: Any governance model must protect against the risks posed by data misuse. Individual perceptions of risks are a subjective function involving individuals' values toward self, family, and society, their perceptions of trust, and their cognitive decision-making skills.

The HIPAA Privacy Rule Puts Some Governance in the Hands of Individuals: Individual privacy protections and individuals' right to choose are codified in the HIPAA Privacy Rule, which attempts to strike a balance between the dual goals of information flow and privacy protection. The choices most commonly given individuals regarding the use of their health information are binary ("yes" or "no") and immutable. Recent federal recommendations and law recognize the need for granular, dynamic choices.

Building a Governance Framework Based in Trust: Avoiding Surprises: Individuals expect that they will govern the use of their own health and genomic data. Failure to build and maintain individuals' trust increases the likelihood that they will refuse to grant permission to access or use their data. The "no surprises principle" asserts that an individual's personal information should never be collected, used, transmitted, or disclosed in a way that would surprise the individual were she to learn about it.

[i]Martin, Blanck & Associates, [ii]Oxford University, [iii]Genetic Alliance

CONTINUED

Fair Information Practices Principles: The FIPPs provide a powerful framework for enabling data sharing and use, while maintaining trust. We introduce the eight FIPPs adopted by the Department of Health and Human Services, and provide examples of their interpretation and implementation.

Reducing Risk through Consumer Engagement: Privacy risk and health risk can be reduced by giving consumers control, autonomy, and transparency, and by engaging them in managing their own health. Explicit "consent" may not always be necessary – the FIPPs offer multiple ways to engender trust and avoid surprises.

Introduction

The provision of safe, high-quality health care and the advancement of biomedical science are highly dependent on the availability of a large volume of personal health information, longitudinally collected, from large populations. The use of health information for these different purposes raises questions about the governance of such data. Governance refers to the collective set of "shared principles, norms, rules, decision-making procedures"[1] that are associated with the collection, storage, use, and dissemination of health information and biospecimens. Individuals contributing the data have a moral claim to be involved in the governance of their personal data based on their autonomy and as a demonstration of respect for them as human beings.[2] This claim is enforced through data protection law and human rights. How to implement this fundamental aspect of governance raises complex decision-making issues for individuals, families, and medical professionals as to what are their rights, duties, and responsibilities in regard to health information in general, and genomic information in particular.

Within the United States, the Health Insurance Portability and Accountability Act (HIPAA)[3] Privacy Rule[4] provides a framework for navigating these requirements. However, the Privacy Rule was largely designed to protect privacy while enabling access for providing and paying for health care services, operating health care enterprises, and protecting public health. The Privacy Rule recognizes the value of health data for other purposes, including research, and defines de identification requirements for enabling these additional uses. However, the Privacy Rule did not consider the special issue of the genome as the ultimate identifier, since few health records contained exome or genome sequences at the time the Privacy Rule was originally crafted. When these legal requirements are implemented in practice, individual choices are often limited and very little information is provided to individuals about their right to govern their information, or about the relevant risks and benefits of sharing it. Thus governance of these data is sometimes mistakenly limited by misapplication of the Privacy Rule.

Volume 4 (2016) Issue Number 2

In any system of governance for health data, short of a property ownership model, trust is a key element. Governance of genomic and genetic data must be built on transparency and accountability to engender trust. Maintaining individuals' trust in an environment of transparency is a core attribute of this governance, and is essential to assuring continuing access to these data. Trust is engendered by respecting individuals' rights and values; treating them fairly; and giving them the information and tools they need to make contextually informed decisions about the use and sharing of their own health information—based on their personal and contextual perception of risk, and at the level of specificity they require. Respecting individuals implies respecting not only their privacy, but also their individual autonomy and right to choose for themselves how they want to manage risk, consistent with their personal values and life situations.

In this paper, we argue that the application of the Fair Information Practices principles offers a framework for governance, and that privacy-enhancing technology that complies with the Privacy Rule and situations when the Privacy Rule does not apply, can offer a dynamic governance tool. In the final section of this paper, we describe a digital platform that enables this model of governance by giving individuals the tools to control how their health information is used, embedded in a trust context, while at the same time respecting individual choice.

Perceptions of Risk

Any governance model must protect against the risks posed by data misuse: infringements upon individuals' and families' rights to privacy; decisions and processes that fail to respond to societal values regarding privacy and data sharing; exposure of individuals to harms, such as social and insurance discrimination based on genetic predisposition; social stratification leading to class disparities; and decisions and processes that weaken societal trust in health care providers and governments.[5] Individual perceptions of these risks are sometimes not an objective or quantifiable quality, but a subjective function involving individuals' values toward self, family, and society; their perceptions of trust; and their cognitive decision-making skills. What seems reasonable and appropriate for one individual may be considered wildly reckless for another. In regard to genomic information, individuals may hold considerably divergent views. Individuals at increased risk for late onset conditions such as Parkinson's or Alzheimer's disease may or may not want to be informed about their susceptibility. Conversely, individuals at increased risk for breast cancer may want to know, in order to take steps to decrease that risk. Across their life spans, individuals are free to exercise their right to be informed (or not to be informed) of their health risks, and to choose a risk-management strategy that is consistent with each individual's life situation and personal values, in the context of their culture and community.

Consciously and subconsciously, individuals continually assess risk and decide how to handle it, based on their individual values and perceived benefits, within the context of their personal experience and the information available to them. A report developed by the President's Council of Advisors on Science and Technology (PCAST)[6] illustrates some of the risks patients consider in deciding whether and how to share their health information:

> Patients are concerned that the storage of their health information in electronic form will make it easier for employers, insurers, government, or malicious electronic intruders to improperly access their records. This concern may make them unwilling to participate in

> health [information technology] systems or [to] grant consent for their information to be used in research, even though the aggregation of patient data to compare treatments and providers is a major benefit of health [information technology]. Data can be anonymized by removing all personal identifiers from the data. But patients also may want to be re-contacted if analysis of their data reveals a problem with a medication they are taking or a treatment that could benefit them.

In reality, very few individuals consider all of their health-related information equally sensitive in all contexts. They may feel quite comfortable allowing their physician to use unencrypted email to remind them of an appointment or to tell them their prescription order has been sent to the pharmacy, but less comfortable receiving the result of a biopsy or genetic test via unencrypted email. Individuals typically desire more granular privacy controls over their health information than is afforded them by yes-or-no consent forms.[7]

The HIPAA Privacy Rule Puts Some Governance into the Hands of Individuals

Within the health care arena, privacy protections and individuals' right to choose are codified in the HIPAA Privacy Rule,[4] which requires that health care providers and health plans obtain individual consent or authorization for various types of uses and disclosures. The specific requirements range from "may obtain consent" (i.e., optional) for uses and disclosures for the purposes of treatment, payment, and health care operations, to written authorization for uses and disclosures of psychotherapy notes. The Privacy Rule attempts to strike a balance between the dual goals of information flow and privacy protection.

> A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule *strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing*.[8] [italics added]

However, the HIPAA Privacy Rule is a complex law whose interpretation and implementation challenge both the organizations seeking to comply and the individuals seeking to understand their rights and protections. As a result, organizations' approaches to compliance with the Privacy Rule sometimes have resulted in practices that comply with the letter of the law, while enabling access and use of individuals' health information in ways these individuals might find surprising or possibly alarming. Transparency is key to avoiding such surprises and reactions. For example, for convenience, some organizations ask individuals to authorize specific uses of their data at the same time they are asked to acknowledge receipt of an already complex Notice of Privacy Practices (NPP). Such a practice may make it difficult for an individual to discriminate between the uses and rights he is being notified about, and uses which he is being asked to authorize.

The complexity of the HIPAA Privacy Rule also leads to organizations' placing a greater emphasis on the procedural governance issues—such as collection, storage, use, and dissemination—than on the governing concept of individuals' rights and protections, which are less well understood. Recent clarifications of these rights from the United States Department of Health and Human Services (HHS) Office of Civil Rights may bolster individuals' ability to better govern access to their own information.[9] Current policies and practices that govern the use and disclosure of individually identifiable health information are designed to enable access for purposes such as treatment, payment, health care

Volume 4 (2016) Issue Number 2

operations, activities preparatory to research, and certain legally required disclosures, while requiring individual, binary ("yes" or "no" to "all" or "none") authorization for other uses. Health care providers and researchers are keenly aware of the uses and disclosures allowed by the Privacy Rule, and can be very creative in devising practices that enable access and use within the bounds of the law. Unfortunately, when making decisions about how their health information is used and disclosed, individuals' choices often are limited to dichotomous choices: "yes" or "no" to use and disclose "all" or "none" of their information for any purpose not permitted or required by the Privacy Rule—and their decisions usually are made with very little information about the relevant risks and benefits of sharing. Furthermore, these choices are usually made once, with no opportunity to change one's choices as circumstances change. The PCAST set forth a proposal for achieving such granular controls, and the Health Information Technology for Economic and Clinical Health (HITECH) Act[10] called for investigation into technologies for segmenting and protecting specific and sensitive individually identifiable information. However, except for psychotherapy notes, the Privacy Rule offers individuals no options for granting permission to use or disclose specific subsets of their health information.

Some uses of health information that the HIPAA Privacy Rule allows without individual authorization may be confusing, surprising, or even suspicious to individuals lacking an understanding of how health care operates. For example, the average patient may not fully understand the full range of activities included under "health care operations" and "preparatory to research." Nor is the average patient likely to know what business associates her provider is using, the services these business associates are providing, or their obligations to protect health information. In fact, even within health care, the term "health care operations" has been inconsistently interpreted, prompting the HITECH Act to enact restrictions on what can be considered "health care operations."

Today's health portals, mobile apps, and online health advisers present new opportunities to engage consumers in improving their own health and in advancing biomedical knowledge. At the same time, these tools present new opportunities to surreptitiously collect and use personal information for purposes relating to "treatment, payment, and health care operations" that the individual may not expect. To increase transparency and possibly avoid surprises, HITECH also added a requirement to maintain an accounting of all disclosures, even for treatment, payment, and health care operations, and a provision that makes business associates directly regulated under HIPAA.

Building a Governance Framework Based in Trust: Avoiding Surprises

Too often health care providers and biomedical researchers view privacy as a barrier to getting access to the data they need; they see their challenge as finding creative ways to obtain the data, while complying with applicable privacy laws and regulations. While legal compliance obviously is necessary, it is not sufficient to build and maintain the perception of responsible stewardship that is essential to gaining an individual's trust that their health information will be collected, accessed and used fairly, respectfully, and responsibly.

Failing to build and maintain the trust of the individuals whose information is needed increases the likelihood that those individuals will refuse to grant permission to access or use their data, if they are asked, or that they will push back mightily if their information is used without their knowledge or consent. A clear example is a federal lawsuit filed by the Texas Civil Rights Project against the Texas

Department of State Health Services and the Texas A&M University System. The lawsuit alleged that the state's failure to ask parents for permission to store and possibly use blood samples collected during newborn screening for birth defects violated constitutional protections against unlawful search and seizure. A settlement reached in 2010 resulted in the destruction of more than 5 million blood samples that, in the typical course of newborn screening for that state, had been "taken from babies without parental consent and stored indefinitely for scientific research."[11] It also undermined the public trust in newborn screening.[12] Newborn screening is arguably the most successful public health program in America, with more than 98 percent of the more than 4 million babies born in the United States annually being screened at birth for several dozen treatable conditions.[13] Nonetheless, clashes between privacy advocates and state public health departments continue to cause the public unease and mistrust.

A study published in 2009 could have predicted such a response from parents. Using an Internet-based survey of a nationally representative sample of parents, the study examined parents' willingness to permit use of their children's newborn-screening blood samples for research with and without the parents' permission. The study found that if the parents' permission was obtained before using the samples, 76 percent were either very willing or somewhat willing to allow their children's bloodspots to be used for research. If the bloodspots were used without the parents' permission, 73 percent were somewhat unwilling or very unwilling to allow their children's bloodspots to be used.[15]

In 1951, Henrietta Lacks's cells were collected without her knowledge or consent; the prolific cells subsequently were used in more than 74,000 studies, many leading to profound insights into cell biology, vaccines, in vitro fertilization, and cancer. The family was never consulted, so they were quite surprised to learn about the marvelous Henrietta Lacks (HeLa) cell line and questioned why no one ever approached them for their consent. Rebecca Skloot, in her book *The Immortal Life of Henrietta Lacks*, very effectively portrayed the family's anguish and confusion over learning of the proliferation of her cells.[16] In 2013, the family was even more surprised to learn that two researchers had used the HeLa cells to sequence her genome and had made it publically available for downloading, again without the family's knowledge or permission.[17] Further, public exposure of the genome presents risk to all of the family members, and they felt even more vulnerable in this very public sharing without their permission. When the Lacks family raised objections, the National Institutes of Health (NIH) acknowledged that they should have sought the family's permission before funding research to sequence the HeLa cell, and NIH then negotiated an agreement with the Lacks family. Terms of the agreement included storage of the genomic data from the two studies in the NIH's database of genotypes and phenotypes, with controlled access to the data and annual reporting of the use of the data. A HeLa Genome Data Access working group, which would include two Lacks family members, would be responsible for reviewing data-access applications, and the cells.[18]

At a workshop convened by NIH to explore scientific and ethical issues related to open access to HeLa genomic data, several Lacks family members clearly articulated their thoughts and requests. They repeatedly expressed their extreme pride in their family's contributions to medical science, and their strong support of the continuing use of the HeLa cell line and genome in biomedical research. They asked only for respect, fairness, and to be kept informed of how the cells and genome are used. As David Lacks explained, the family came up with the idea of governance in the form of controlled access so

Volume 4 (2016) Issue Number 2

that they "wouldn't be surprised," while still allowing his grandmother's genome to be used to advance medical science. As one participant pointed out, the family's requests are highly consistent with the Fair Information Practices Principles that for decades have been used throughout the world to guide the fair use of personal information.[19] The use of the cells is now governed by a family advisory board in collaboration with NIH.[20]

Trust is built through experience. When consumers are surprised to learn that their personal information has been collected, used, or disclosed in ways they were unaware of, did not approve of, and did not expect, their trust is eroded. Individuals expect that they will govern the disclosure of their health information. This concept is sometimes referred to as the "no surprises principle"—an individual's personal information should never be collected, used, transmitted, or disclosed in a way that would surprise the individual were she to learn about it. Every time an individual is surprised to learn that a trusted caregiver has shared her health information with someone whom she did not expect to see it, or used her information in research without her permission, trust is eroded. At the same time, the risk that the unauthorized use will be exposed in ways that will affect the perceptions and behaviors of the broader public is elevated. Every caregiver and researcher whose success depends on the availability of high-quality health information should assiduously act in accordance with the "no surprises principle." If an individual is likely to be surprised to learn that his information is being collected, used, or disclosed in the way contemplated, then his permission should first be obtained—even if the law does not require the individual's consent.

England's National Health Service (NHS) learned the importance of the "no surprises principle" the hard way. The NHS had high aspirations when it decided to build a national database of individuals' health information. Having access to such an extensive repository would allow researchers to investigate drug side effects and patient outcomes, thus facilitating medical advances and ultimately saving lives. Building such a database was legal; the data were pseudonymized, and all individuals were given the opportunity to opt out. Unfortunately, the NHS's plans were not effectively communicated to the public—resulting in a "surprised" public and attendant mistrust of the NHS. As a result of public outcry, the NHS was compelled to delay the program to permit "more time to build understanding of the benefits of using the information, what safeguards are in place, and how people can opt out if they choose to."[21]

Researchers fear that if health information is not freely accessible, it cannot be used to advance biomedical knowledge. A general perception in the research community is that if researchers ask individuals for permission to use their information, and allow them to establish highly granular, context-specific access rules that they can change at any time, biomedical research will at best be skewed by selection bias and at worst grind to a halt. Our hypothesis is that an engaged public will participate in research at a much higher rate than the current 4 percent or 5 percent enrollment in clinical trials, and that any improvement in this enrollment rate will result in *less* selection bias.

Fair Information Practices Principles

Several decades ago, recognition of the futility of anticipating every questionable or evasive method that might be used, combined with an appreciation of the multidimensionality of trust, led to the development of a set of principles for responsible information stewardship, which is essential to establishing and maintaining public trust when collecting, using, disclosing, and sharing personal information. The Fair Information Practices Principles

(FIPPs) were first published in 1973 as the *Code of Fair Information Practices*[22] and became the basis for the United States federal Privacy Act of 1974.[23] In more recent years, these principles were adopted by the HHS as the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*[24] and by the White House as a Consumer Privacy Bill of Rights to serve as a code of conduct for companies conducting business on the Internet.[25] The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) also have published similar principles as *Generally Accepted Privacy Principles*.[26]

These principles provide a powerful framework for enabling data sharing and use, while maintaining trust. The FIPPs included in the HHS guidance comprise the following eight principles, which have been implemented in the HIPAA Privacy Rule or related statutes and have led to the development of governance practices to implement the principle. Each principle has been adopted by the HHS as guidance for health care entities who electronically exchange individually identifiable health information,[24] and is followed by interpretation, examples, and where applicable, examples of how the principle has been translated, and possibly expanded, in law.

1. Individual Access: Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
   The HIPAA Privacy Rule gave individuals the right to inspect and obtain a copy of their own health information; the HITECH Act further provided that, at the individual's request, the information must be provided electronically to either the individual or to a third party named by that individual in the format requested by the individual.[9] The Clinical Laboratory Improvement Amendments (CLIA) rule enacted in February 2014 expanded this provision further to include the right for a patient to obtain laboratory test results directly from the lab.[27] Any entity that holds health information about an individual should provide the capability for that individual to access and obtain a copy of his or her own information in either print or electronic form, in the format requested.
2. Correction: Individuals should be provided with a timely means for disputing the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
   Any entity that holds health information about an individual should provide the capability for that individual to point out errors and to request that the errors be corrected. If the entity concludes that no changes are warranted, the individual's dispute should be recorded. The Consumer Privacy Bill of Rights[25] states that consumers have a right to access and correct personal data in accordance with the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.
3. Openness and Transparency: There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and their individually identifiable health information.
   Consumers should be able to trust that their health information will be collected, used, and disclosed only in ways that are consistent with their expectations for a given context. This principle embodies the "no surprises principle" discussed above—an individual's health information should never be collected, used, transmitted, or disclosed in a way that would surprise the individual were he to learn about

it. If an individual would likely be surprised, then permission should first be obtained. For example, after a nurse has drawn a blood sample, patients are unlikely to be surprised to learn that their name and birthdate have been sent to a laboratory along with the sample. However, they might be very surprised to learn that the laboratory uses the blood sample for purposes other than running the test the doctor has ordered. This principle is particularly relevant with respect to Internet-based services and social networking applications, which often surreptitiously collect information about the user's actions as a means of "customizing the user experience"—which may be to the good or detriment of the individual. Consumers have a right to easily accessible and understandable information about privacy- and security policies and practices, including the use of technologies that collect information about users and their actions, outside the user experience.

4. Individual Choice: Individuals should be provided with a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.
   Key concepts here are "choice" and "informed." Not only do individuals have the right to decide what personal information is collected and how that information may be used and disclosed, they also have the right to be informed of both the risks and potential benefits associated with their decision. Whether an entity uses an opt in, opt out, or open choice, the individual must be given the opportunity to make that choice before the action in question has been taken—in sufficient time for it to be meaningful.
   Today, "individual choice" is generally presented to the individual at a given point in time, in the form of a printed "consent" document that the consenter signs by hand that is then filed away for safekeeping. Individual choice needs to be an ongoing activity through which an individual expresses her wishes and preferences with respect to the use of her personal information. A single consent document cannot bear the burden of what must be a much fuller, ongoing engagement. A one-time consent form allows only a brief snapshot of an individual's health status and values, and not the longitudinal engagement of an individual over time, health conditions, and changing priorities and values. "Individual choice" must be viewed as being a dynamic, ongoing process that occurs within the context of the full set of fair information practices.
5. Collection, Use, and Disclosure Limitation: Individually identifiable health information should be collected, used, and disclosed only to the extent necessary to accomplish a specified purpose and never to discriminate inappropriately.
   In security engineering, this is known as the "principle of least privilege,"[28] which means that each user, software program, and process should be able to authorize use of only the information, resources, and privileges necessary to fulfill its assigned responsibilities. For the HIPAA Privacy Rule, it is the "minimum necessary" standard, which includes minimizing the access authorized for each person within an organization, minimizing the amount of information that is disclosed when disclosure is necessary, and minimizing the amount of information that is requested. The introduction of genomic and genetic information into health care and biomedical research raises the stakes for those seeking to limit the use of identifiable information since the individual genome is inherently the ultimate "biometric identifier"—one of the 18 data elements the HIPAA Privacy Rule enumerates as individual identifiers.

6. Data Quality and Integrity: Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes, and that it has not been altered or destroyed in an unauthorized manner. Technical security safeguards are available to protect information from accidental and malicious alteration and to detect when data have been corrupted. This principle goes a step further to say that an organization has a responsibility to help ensure that each individual's health information is complete, accurate, and current. This means, for example, that all of the information an entity holds for a given individual can be associated with the same identity.
7. Safeguards: Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. The HIPAA Security Rule[29] defines administrative, technical, and physical safeguards designed to protect the confidentiality of information, the integrity of data, and the availability of resources. The Security Rule is strongly grounded in risk assessment and risk management. Entities should assess risks on an ongoing basis to identify new vulnerabilities and to assure that their security safeguards can adequately protect against new and emerging threats.
8. Accountability: These principles should be implemented, and adherence assured, through appropriate monitoring, and other means and methods should be in place to report and mitigate nonadherence and breaches. Entities should make these principles part of their governance process so that adherence is continuously monitored and any policy breaches are detected and corrected. The HIPAA Security and Privacy Rules call for two types of accountability: the Security Rule requires the recording and review of a system audit trail, and the Privacy Rule requires maintaining an accounting of all disclosures of protected health information. An audit trail records security-relevant events, such as logon attempts, launching a software program, and creating a record in a database, while an "accounting of disclosures" records information about the release of health information from one organization to another. Both system audit trails and disclosure logs will be useful in monitoring adherence with these principles.

Reducing Risk Through Consumer Engagement

Privacy risk and health risk can be reduced by giving consumers control, autonomy, and transparency, and by engaging them in managing their own health. Adhering to the FIPPs helps reduce individuals' privacy risk by giving them greater visibility into how their information is accessed, used and shared—reducing the likelihood of surprises. Consistent with the "no surprises principle," individuals should not be surprised to learn that their health information is being disclosed or used in any particular way. Explicit consent may not always be necessary—the FIPPs offer multiple ways to engender trust and avoid surprises. One might speculate how the outcomes of some of the scenarios cited in this paper might have been different had the affected parties been engaged in the decision-making and kept informed of actions thereafter—specifically, the Texas A&M newborn screening program, NHS national health database, and the use of HeLa cells. Authentic engagement in the health care setting, such as peer-to-peer outreach or social networking among patients involved in clinical trials, or personal notification of the use of health information in observational studies, can help avoid surprises.

Volume 4 (2016) Issue Number 2

Health care professionals, biomedical researchers, and consumers are broadly recognizing the value of engaging individuals in improving their own health and the health of their families, and in helping to advance biomedical science. Today's mobile technology, social networking, consumer health technology, ubiquitous connectivity, and powerful search capabilities provide consumers with the tools they need to engage in health advancement to whatever extent, using whatever means, they wish. However, consumers' willingness to participate in advancing biomedical science at the highest level can be thwarted by the research enterprise's almost exclusive reliance on consent as the single mechanism for engagement. Confining the interaction between the individual and biomedical research to a single transaction—signing a consent form—denigrates what could be a robust engagement, and limits the opportunity to create and nurture a more scientifically and medically literate populace. Longitudinal engagement, within the context of fair information practices, enables the collection of genomic, clinical, environmental, and lifestyle data critical to making headway in prevention, diagnoses, and interventions.

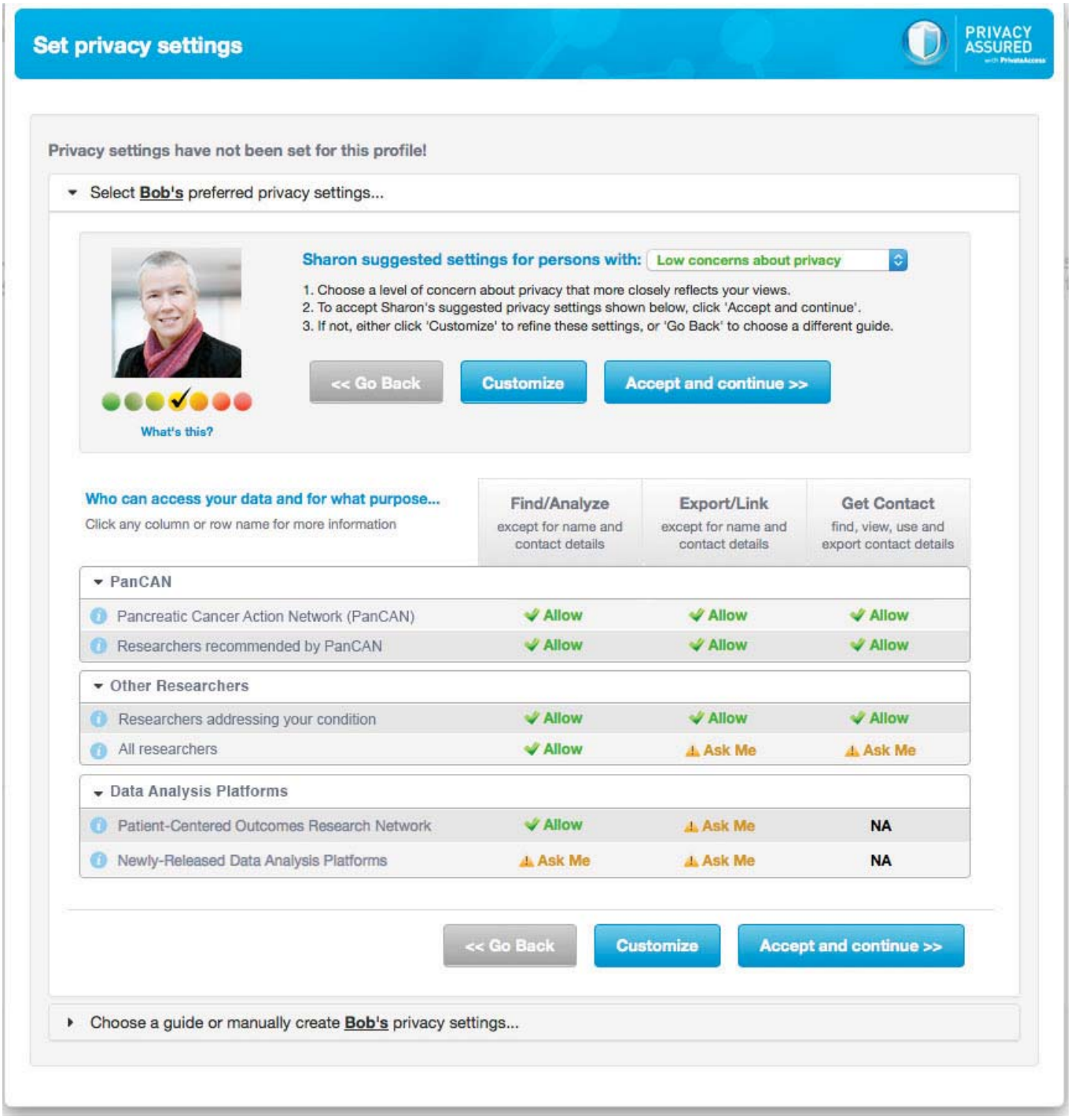
Platform for Engaging Everyone Responsibly (PEER)

The Platform for Engaging Everyone Responsibly (PEER)[30] is a technology solution that enables individuals to govern the access to and use of their health information. Using FIPPs as a basis, Genetic Alliance and Private Access Inc. are collaborating on an initiative that enables individuals to participate in advancing medical science, while protecting individuals' privacy consistent with their own perceptions of risks and benefits. PEER includes a repository of health information that is made discoverable and accessible to authorized researchers only in accordance with permissions established by the individual participants who contribute their information.[31] At present 40 communities (e.g., disease advocacy organizations, health provider professional societies, special interest groups) use PEER to build registries, cohorts, and campaigns. Approximately 10,000 individuals are sharing their health information through PEER. This information includes self-reported health information, electronic health record (EHR) data, genetic test reports, and (soon) genomes and exomes. Permissions can be very granular and specific (e.g., "only my de-identified data may be included in searches, and only for clinical trials for drugs to treat type 1 diabetes") or very liberal (e.g., "all of my identifiable data may be used for any research") or something in between (e.g., "my linked data may be discovered by diabetes researchers who may then ask PEER to contact me").

Participants make their health information available and establish their privacy preferences through a PEER interface that uses a simple, interactive, gamified survey to collect answers to questions using common data instruments provided by Genetic Alliance and many instruments created by the sponsoring community. PEER was created on the premise that each FIPP is critical, and that the experience must be local, centered in a trusted community. Thus, participants can view short videos of members of their community, human guides, each offering suggestions for privacy settings corresponding to the guide's own perceptions of high, medium, and low risk-benefit ratios (Figure 1). An individual may change her privacy permissions at any time, and as often as she wishes. Regardless of how a participant may choose to set her privacy permissions, the system provides defense-in-depth security protection for all of the data entrusted to PEER.

Contact information, privacy and sharing preferences, and health information are held in three separate databases, with Genetic Alliance

Figure 1. Guides Offer Three Levels of Suggested Privacy Settings



Volume 4 (2016) Issue Number 2

responsible for health information, and Private Access holding responsibility for contact information and privacy settings (Figure 2). All data are encrypted for both storage and transmission, and a participant may view his information and an audit trail of accesses at any time. Genetic Alliance's Ethics Team[32] provides ethical, legal, and policy oversight. Western Institutional Review Board (IRB) has approved the PEER system itself,[33] and various IRBs, including the Genetic Alliance IRB, have approved specific projects that use PEER.

PEER exemplifies a system that empowers individuals to manage their own health information consistent with their personal values and those of their community, their tolerance of perceived risks, and their own desire for specificity and autonomy. The online tools, information, and guidance that PEER offers convey respect for each individual's personal values while enabling everyone to participate in advancing medical research. As shown in Figure 3, PEER applies the principles of fair use, no surprises, and consumer engagement to help advance biomedical science. PEER's strict adherence to the FIPPs creates an environment designed to engender trust for all participants. PEER's privacy policy also details this and can be viewed at peerplatform.org/privacy. This adherence is largely managed through the system and does not rely on the data seekers, the researchers, and investigators to manage the governance. Interested researchers and clinicians apply for an account, and after their credentials are examined, they are given access to any data that individuals have given them permission to see or use, including contact information. The governance is in the hands of the individuals. At present, we do not have universal return of results and notification.

Figure 2. PEER Stores Individual Contact Information, Privacy and Sharing Preferences, and Health Data in Three Separate Data Bases

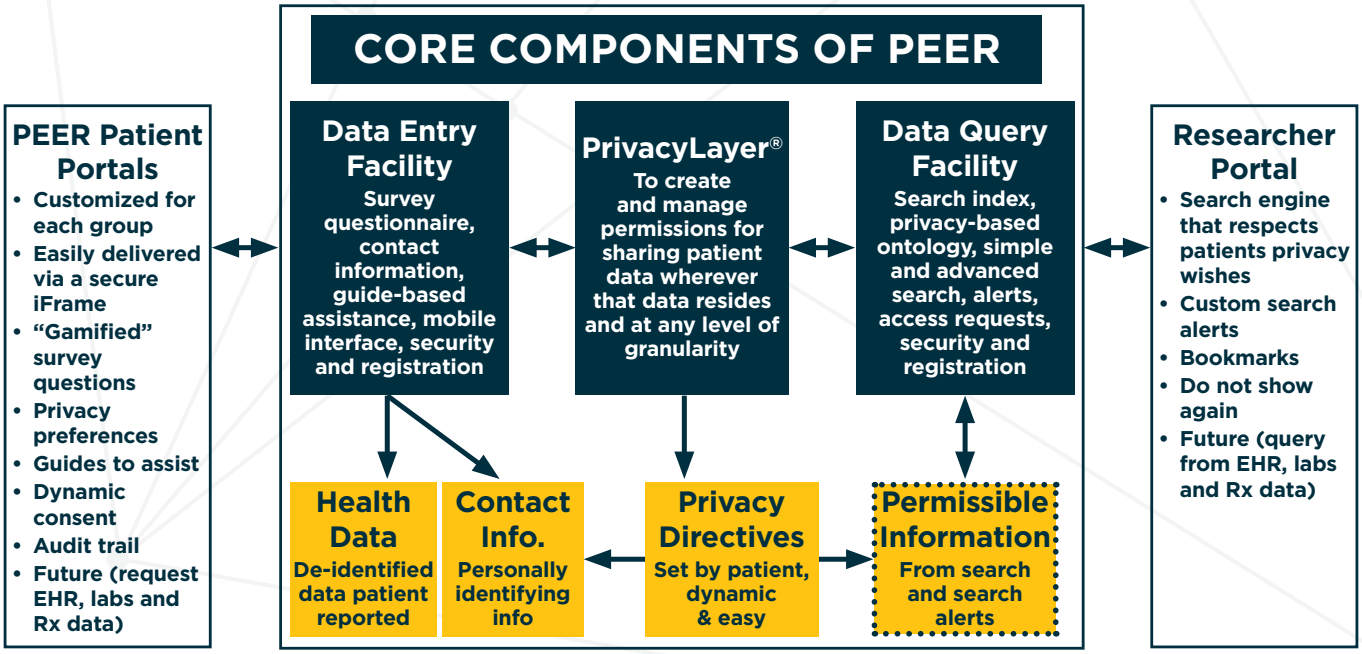


Figure 3. PEER Conforms to the Fipps to Engage Consumers in Medical Research

FAIR INFORMATION PRACTICES PRINCIPLE	PEER CONFORMITY TO PRINCIPLE
1. Individual Access	All data held by PEER are contributed by the individual to whom the data pertain. Participants contribute data through surveys, by uploading documents (e.g., BRCA test results), or by asking their physician to transmit EHR data to PEER's Direct address. Participants always have access to all of their own data.
2. Correction	All data held by PEER were contributed by the individuals to whom the data pertain. Participants can go back to prior answers and correct them. Answers are time-stamped, and both answers are available to the data seeker. Participants can also modify privacy and sharing preferences to make them "correct" with respect to the individual's current values, sensitivities, and priorities. Assuring that survey questions are objective and free of value judgments has been a critical issue for PEER. We have worked with the communities that sponsor portals: first to access how to ask value-based questions, then to use multiple reviewers in the coding process to reduce bias.
3. Openness and Transparency	Participants are able to see all of their own data and their own sharing preferences. In addition, participants are able to see how their own responses compare to the responses of others (who allow their data to be used in this way), and how their own responses change over time. Participants are also able to view an audit trail of accesses to their data at any time. All of the data-seeker agreements authorizing use of PEER are governed by the principle that, if use of the data results in findings of health importance to the individual, this information is communicated back to the individual.
4. Individual Choice	Health information is held in PEER and is accessed and used only within the parameters of authorization that are assigned by the individual and in force at the time of access. The individual can change authorizations over time, but changes made after the information has been exported and used outside the PEER system are not governed by new preferences. PEER manages authorizations to data at a granular level. Various classes and roles for data seekers are established, and access to data is limited to those individuals and organizations whose profiles conform to the applicable access authorization rules with regard to discovery, use, and export of data, and sharing of contact information.
5. Collection, Use, and Disclosure Limitation	This FIPP protects participants from sharing more than they need to share for a researcher to answer a question, and the inferences that can be made from use of the data. PEER gives the individual the tools to define rules governing the discovery, use, and export of data, and for the participant to be contacted. Thus the participant controls the minimum and maximum access for different types of data and for different categories of data seekers. This approach acknowledges that various people have different sensitivities about what constitutes minimum and maximum. To limit the scope and associativity of sensitive information held by PEER, information is stored separately in three databases: (1) contact information, (2) privacy and sharing preferences, and (3) health information. Identities are made known to data seekers only as authorized by the individuals to whom the data pertain.

Volume 4 (2016) Issue Number 2

Figure 3. PEER Conforms to the Fipps to Engage Consumers in Medical Research (Cont'd)

FAIR INFORMATION PRACTICES PRINCIPLE	PEER CONFORMITY TO PRINCIPLE
6. Data Quality and Integrity	The data held by PEER is of several types—participant-reported data, electronic health record (EHR) data, and genomic-related data. The accuracy of the participant-reported data is as high as the participant chooses to make it. Certain fields are constrained to prevent inaccuracies such as completely unrealistic weights and heights. For the EHR data that is extracted into the system, we believe that PEER helps enhance the quality because if the patients can see the data, they will be more likely to report inaccuracies to their providers. This assumption is untested. Genomes and exomes are only as accurate as the sequencing so PEER has no way in the short run to test their accuracy.
7. Safeguards	The identity of all PEER users is verified before they are given an account as a participant or data seeker. PEER screens data seekers and requires that their credentials meet a minimal threshold. In addition, rights to use the data are revoked if the data seeker is found to be misusing PEER data. Two-factor authentication is used at login time. Participants are able to access their own data and the data of other accounts linked to their own. Data seekers are able to access only data for which they have been authorized. All data are encrypted for both storage and transmission. All security-relevant activity in the system is recorded in the audit trail. Sensitive data are segmented into three separate databases, thus limiting disclosure and privacy (associativity) risk.
8. Accountability	All accesses to data are recorded in the audit trail. State-of-the-art security monitoring of the infrastructure is performed by a third party.

Conclusion

While many discussions of governance are concerned primarily with health information after it has been collected from the individuals, governance must begin with the individual's overseeing the contribution and use of this information. Current policies and practices that govern the use and disclosure of individually identifiable health information are designed to enable access for purposes such as treatment, payment, health care operations, activities preparatory to research, and certain legally required disclosures, while requiring individual, binary ("yes" or "no" to "all" or "none") authorization for other uses. Health care providers and researchers are keenly aware of the uses and disclosures allowed by the HIPAA Privacy Rule without the individual's authorization, and can be very creative in devising practices that enable access and use within the bounds of the law. Both providing safe, high-quality health care and advancing biomedical science are highly dependent on the availability of large volumes of health information, longitudinally collected, from large populations of individuals. Maintaining individuals' trust in an environment of transparency is essential to assuring continuing access to these data. Trust is engendered by respecting individuals' rights and values, treating them fairly, and giving them the information and tools they need to make dynamic, contextual, informed decisions about the use and sharing of their own health and genomic information, based on their personal perceptions of risk, and at the level of specificity they require. Maintaining trust requires assiduous adherence to the Fair Information Practices Principles.

Acknowledgements

We acknowledge the work of Robert Shelton and Private Access. In addition, we also recognize the Genetic Alliance Staff and the Genetic Alliance Think Tank for their contributions. JK is funded by Wellcome Trust Award 096599/2/11/Z.

References

1. Drake WJ in Bygrave LA. *Internet Governance by Contract*. Oxford University Press. 2015. ISBN: 9780199687343
2. Beyleveld D and R Browsword. *Human Dignity in Bioethics and Biolaw*. Oxford University Press. 2002. ISBN: 9780198268260
3. US 104th Congress. Federal Register. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. Available from http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (accessed 3/21/16).
4. US Department of Health and Human Services. The HIPAA Privacy Rule. Available from http://www.hhs.gov/hipaa/for-professionals/privacy/ (accessed 3/21/16).
5. OECD. *Health Data Governance: Privacy, Monitoring and Research*, OECD Health Policy Studies, OECD Publishing, Paris. 2015.
6. US Presidents Council of Advisors on Science and Technology. Realizing the full potential of health information technology to improve healthcare for Americans: The path forward [document on internet]. 2010 [cited 2013 Mar 13]. Available from: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf (accessed 3/21/16).
7. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. *JAMIA*. 2013 Jan; 20(1): 7-15.
8. US Department of Health and Human Services. Summary of the HIPAA Privacy Rule. Available from http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ (accessed 3/21/16).
9. US Department of Health and Human Services. Individuals' right under HIPAA to access their health information 45 CFR §164.524. Available from http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/ (accessed 3/21/16).
10. US Congress. American Recovery and Reinvestment Act of 2009. Health information technology for economic and clinical health. 2009. Available from: http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf (accessed 3/21/16).
11. Root J. Texas officials agree to destroy babies' blood samples after settling lawsuit. Texas Civil Rights Project. February 14, 2010. Available from: http://www.texascivilrightsproject.org/1822/texas-officials-agree-to-destroy-babies-blood-samples-after-settling-lawsuit/ (accessed 3/21/16).
12. The Baltimore Sun. Stored newborn blood samples raise concern. April 6, 2011. Available from http://articles.baltimoresun.com/2011-04-16/health/bs-hs-baby-blood-samples-20110416_1_samples-parents-support-genetic-disorders (accessed 3/21/16).
13. Therrell BL, CD Padilla, JG Loeber, et al. Current status of newborn screening worldwide. *Semin Perinatol*. 2015 Apr;39(3):171-87. doi: 10.1053/j.semperi.2015.03.002.
14. Arnold CG. Two faces of patient advocacy: the current controversy in newborn screening. *J Med Ethics*. 2014 Aug;40(8):558-62. doi:10.1136/medethics-2012-101019. Epub 2013Apr 16. PubMed PMID: 2592379.
15. Tarini BA, et al. Not without my permission: Parents' willingness to permit use of newborn screening samples for research. Public Health Genomi. 2009. Available from http://www.cchfreedom.org/pr/tarini_biobanking%20paper_parent%20attitudes.pdf (accessed 10/11/2015).
16. Skloot R. *The immortal life of Henrietta Lacks*. New York: Random House; 2009.
17. Skloot R. The immortal life of Henrietta Lacks, the sequel. *The New York Times*. Sunday Review. March 23, 2013. Available from http://www.nytimes.com/2013/03/24/opinion/sunday/the-immortal-life-of-henrietta-lacks-the-sequel.html?_r=0 (accessed 3/21/16).
18. Zimmer C. A family consents to a medical gift, 62 years later. The New York Times. 2013 Aug 07 [cited 2014 May 19]. Available from: http://www.nytimes.com/2013/08/08/science/after-decades-of-research-henrietta-lacks-family-is-asked-for-consent.html?pagewanted=all&_r=0 (accessed 3/21/16).
19. Baker D. NIH workshop on scientific and ethical issues related to open-access HeLa genomic data [unpublished conference notes]. Washington, DC: National Institutes of Health; 2014 May 14.
20. McManus R. NIH restricts access to Henrietta Lacks genomic data. *NIH Record*. August 30, 2013. Available from https://nihrecord.nih.gov/newsletters/2013/08_30_2013/story2.htm (accessed 3/21/16).
21. Walker P, J Meikle and R Ramesh. NHS in England delays sharing of medical records. February 18, 2014. Available from: http://www.theguardian.com/society/2014/feb/18/nhs-delays-sharing-medical-records-care-data (accessed 3/21/16).
22. US Dept. of Health, Education and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. Records, computers, and the rights of citizens. July 1973. Available from http://www.justice.gov/opcl/docs/rec-com-rights.pdf (accessed 3/21/16).
23. Electronic Privacy Information Center. The Privacy Act of 1974. 5 U.S.C. 552a. US Congress; 1974. Available from https://epic.org/privacy/1974act/ (accessed 3/21/16).
24. US Department of Health and Human Services. Nationwide privacy and security framework for electronic exchange of individually identifiable health information. Office of the National Coordinator for health Information Technology; 2008. Available from https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (accessed 3/21/16).
25. United States. Consumer data privacy in a networked world: A framework for protecting intellectual property privacy and promoting innovation in the global digital economy. Washington DC: White House; 2012. Available from https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed 3/21/16).

26. American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants. Generally accepted privacy principles. August 2009. Available from http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_PRAC_%200909.pdf (accessed 3/21/16).
27. United States. Federal Register. CLIA Program and HIPAA Privacy Rule; Patients access to test reports. Available from: https://www.federalregister.gov/articles/2014/02/06/2014-02280/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports (accessed 3/21/16).
28. Massachusetts Institute of Technology. Basic principles of information protection. Available at http://web.mit.edu/Saltzer/www/publications/protection/Basic.html (accessed 3/21/16).
29. Genetic Alliance. Platform for engaging everyone responsibly. Available from http://www.geneticalliance.org/programs/biotrust/peer (accessed 3/21/16).
30. US Department of Health and Human Services. Federal Register. 45 CFR Parts 160, 162, and 164: Health Insurance Reform: Security; Final Rule. Feb 20, 2003. Available from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf (accessed 3/21/16).
31. Terry SF, R Shelton, G Biggers, D Baker, and K Edwards. The haystack is made of needles. *Genetic Testing and Molecular Biomarkers*. 2013 March; 17(3)175-177.
32. Genetic Alliance. Ethics Team. Available from: http://www.geneticalliance.org/programs/biotrust/ethicsteam (accessed 3/19/2016).
33. Western Institutional Review Board [Internet]. [Cited 2014 Jul 03]. Available from: https://www.wirb.com/Pages/default.aspx (accessed 3/21/16).