Article published online: 2021-11-15

A Policy Framework to Support Shared Decision-Making through the Use of Person-Generated Health Data

Carolyn Petersen[1] Margo Edmunds[2] Deven McGraw[3] Elisa L. Priest[4] Jeffery R.L. Smith[5] Eagan Kemp[6] Hugo Campos[7]

[1] Mayo Clinic, Rochester, Minnesota, United States
[2] AcademyHealth, Washington, Dist. Of Columbia, United States
[3] Ciitizen, Corp., Palo Alto, California, United States
[4] Baylor Scott and White Health, Dallas, Texas, United States
[5] Office of the National Coordinator for Health IT, U.S. Department of Health and Human Services, Washington, Dist. Of Columbia, United States
[6] Public Citizen, Washington, Dist. Of Columbia, United States
[7] All of Us Research Program and California Precision Medicine Consortium (CaPMC), Oakland, California, United States

Address for correspondence Carolyn Petersen, MS, MBI, FAMIA, Mayo Clinic, 200 First Street, SW, Rochester, MN 55905, United States (e-mail: petersen.carolyn@mayo.edu).

ACI Open 2021;5:e104–e115.

Abstract

Background Individuals increasingly want to access, contribute to, and share their personal health information to improve outcomes, such as through shared decision-making (SDM) with their care teams. Health systems' growing capacity to use person-generated health data (PGHD) expands the opportunities for SDM. However, SDM not only lacks organizational and information infrastructure support but also is actively undermined, despite public interest in it.

Objectives This work sought to identify challenges to individual–clinician SDM and policy changes needed to mitigate barriers to SDM.

Methods Two multi-stakeholder group of consumers, patients, caregivers; health services researchers; and experts in health policy, informatics, social media, and user experience used a consensus process based on Bardach's policy analysis framework to identify barriers to SDM and develop recommendations to reduce these barriers.

Results Technical, legal, organizational, cultural, and logistical obstacles make data sharing difficult, thereby undermining use of PGHD and realization of SDM. Stronger privacy, security, and ethical protections, including informed consent; promoting better consumer access to their data; and easier donation of personal data for research are the most crucial policy changes needed to facilitate an environment that supports SDM.

Conclusion Data protection policy lags far behind the technical capacity for third parties to share and reuse electronic information without appropriate permissions, while individuals' right to access their own health information is often restricted unnecessarily, poorly understood, and poorly communicated. Sharing of personal information in a private, secure environment in which data are shared only with individuals' knowledge and consent can be achieved through policy changes.

Keywords
- health policy
- policy making
- privacy
- patient engagement
- health care reform
- data management

received
August 16, 2020
accepted after revision
September 9, 2021

DOI https://doi.org/10.1055/s-0041-1736632.
ISSN 2566-9346.

Georg Thieme Verlag KG, Rüdigerstraße 14, 70469 Stuttgart, Germany

Introduction

Shared decision-making (SDM) is a process of engagement that balances patient preferences and values with clinical evidence in the service of better delivering person-centered health care.[1–3] Despite the growing importance of SDM strategies and tools to patients and health care systems, structural and cultural barriers related to data management hinder proactive use of such strategies and tools. Patients have long relied upon clinicians to manage personal information generated during clinical encounters, and will continue to do so even as they gain access to personal health information (PHI) through eHealth tools such as patient portals and application programming interfaces (APIs). The growing use of consumer-friendly devices (e.g., wearables) is making it possible for patients to generate health-related data that both they and their care teams can use to facilitate better health. However, technical barriers, legislative and regulatory constraints, and market forces currently prevent realization of the potential of person-generated health data (PGHD). This paper describes conditions in the United States (U.S.) that currently limit the use of PGHD in SDM and recommends strategies to remove these barriers.

Definition of Terms

Person-Generated Health Data (PGHD) are health-related data created, recorded, gathered, or inferred by or from patients or their designees to help address a health concern.[70]

Shared Decision Making (SDM) is an approach where clinicians and patients share the best available evidence when faced with the task of making decisions, and where patients are supported to consider options, to achieve informed preferences.[71]

Approach to This Work

With funding from a Eugene Washington Patient-Centered Outcomes Research Institute (PCORI) Engagement Award to AcademyHealth, 50 diverse stakeholders with expertise in consumer-generated health data were invited to help develop a unifying framework for using PHI in SDM with care teams. The purpose of the framework was to develop a consumer-driven, consensus-based research agenda to guide future studies that would: (1) strengthen the evidence base on using consumer-generated information in SDM; (2) identify policy barriers and changes needed to facilitate SDM; and (3) describe the tools, culture, and organizational changes needed to support and encourage SDM (e.g., addressing time pressures). This approach was based on Eugene Bardach's widely-used policy analysis framework, which describes a systematic, multidisciplinary process for evidence-based, consensus-based decision-making about complex multisector issues.[4,5]

Participants

Guided by a representative advisory group, two multi-stakeholder workshops were held in the spring of 2019 in Washington, DC, and at the University of California-Davis in Sacramento, California. Stakeholders were invited by the advisory group based on their expertise and experience with consumer informatics and digital health; conducting, funding, and participating in research on patient-centered outcomes and SDM; health policy; and health communications. They included consumers, patients, caregivers, clinicians, policy experts, health services researchers, epidemiologists, and experts in social media, graphic design, and user experience and came from academia, non-profit research and membership organizations, health care delivery systems, and public and private sector funders. Several had previously participated in PCORI-funded studies or convenings on consumer informatics and electronic health data and were suggested through advisory group members, the project team, and PCORI. They also reflected diversity in racial, ethnic, and gender identities.

The advisory group (named in the Acknowledgments) was co-chaired by a consumer and an informatics researcher; its members included three consumer-caregivers, three health systems researchers, and an experience design strategist. All of the consumers and patients had lived experience with managing health conditions and using electronic health data through web portals, registries, and PGHD (e.g., wearables, implants), and several were active in social media. The advisory group members reflected diversity in racial/ethnic and gender identities. Honoraria were provided and travel expenses were paid for participating consumers and advisory group members.

Method

The approach followed the steps described in Bardach's policy analysis framework: (1) Define the problem; (2) Assemble the evidence; (3) Construct policy alternatives; (4) Select the criteria for decision-making; (5) Project the outcomes; (6) Confront trade-offs; (7) Make decisions/recommendations; and (8) Share the results of the process. The 1.5 day workshop structure included background pre-readings based on peer-reviewed literature selected by the project team and advisory group; facilitated, interactive group participation in large and small groups to define the problem and set priorities for discussion; and real-time development and sharing of written outlines and visual designs to illustrate key concepts during the workshop. A collaborative consensus approach was used in which a variety of stakeholder perspectives were represented and all perspectives were discussed and valued equally during the deliberations.

Through facilitated discussions and interactive group participation, all participants engaged in group priority-setting by consensus and came to agreement about high-level priorities for four key topics for recommendations: gaps in the evidence base on SDM; the informatics tools used in PGHD; policy facilitators and barriers to sharing PHI; and the cultural changes that would be needed to support implementation of SDM on a larger scale.

After the workshops, four volunteer cross-sector writing teams were formed to write papers for submission to peer-reviewed journals. Each paper was led by an advisory group member and included at least one consumer/caregiver representative along with interested research, policy, and technology experts for each of the four topics. The entire advisory group continued to meet on a monthly basis for 5 months to refine the conceptual framework; standardize definitions across the papers; review illustrative graphic designs; and discuss cross-cutting themes in the recommendations. The four papers were submitted separately to peer-reviewed journals in late fall 2019.

Background

Consumer interest in using technology to monitor and treat health conditions is growing,[6,7] along with interest in connecting and sharing PHI with other individuals undergoing similar experiences.[8–10] Most often, consumers prefer to share their information in a secure environment in which their information will be available to them and other authorized users, such as their clinicians and caregivers, when needed but protected from unauthorized use and breaches.[11]

When important and relevant health information is not readily available through clinical channels, or when information is incomplete or inaccessible, consumers often turn to social media platforms to learn more about a condition, share information, find out about new clinical trials and treatments, rate clinicians, and generate a myriad other types of information that is not collected, studied, or otherwise available through clinical sources.[11–14] Data from online sources such as Facebook, Google, and Twitter are now used for research on health habits, treatment preferences, and recruitment into clinical studies, providing important sources of PGHD but raising questions about informed consent, privacy, and other ethical issues.[12,13,15]

The importance of electronic health records and decision support tools in improving patient safety and health care was one of the main drivers for the 2009 Health Information Technology for Economic and Clinical Health (HITECH) legislation, which provided financial incentives for clinicians, hospitals, and health systems to adopt electronic health records.[16] At the time, it was hoped that building a standard-based, interoperable electronic information infrastructure would make it easier to share electronic information among providers to coordinate care for patients as they moved through the continuum of care.[17]

There are some prominent examples of health system changes to promote electronic information exchange. More than 200 health systems are now participating in OpenNotes, which allows 40 million patients to access their clinicians' visit notes electronically through patient portals.[18,19] Patients who access their clinical visit notes are more likely to manage their medications appropriately, experience greater trust in their providers, and feel more satisfied with their quality of care.[20–23] However, the majority of health systems lack the capacity or inclination to share clinical information with other health systems, out of technical, legal, or business concerns.[24]

Data Sources and Potential Sites of Delivery

The rapid emergence of smartphones and other new technologies, particularly consumer-facing technologies such as wearable health/fitness trackers, has resulted in a rapidly evolving landscape of both data sources and data types.[25] The majority of health data no longer reside in electronic health records,[26] and many of these data can be used to infer health or factors that influence health. Data that are generated with intention by consumer devices, such as exercise and sleep data, are well-known and familiar, but other less familiar types of data include patient-reported outcome measures used to record experiences with investigational therapies and/or established treatments, signals from in-home motion detection systems that indicate when individuals are not undertaking their usual activity levels, mobile health apps that remind users to take their medication and record that they have done so, Web search metrics that suggest the spread of infectious disease, social media posts that reveal an increase in mental health concerns in response to public events, and others.[27]

Besides these recognized forms of data, the use of devices leaves behind a trail—so-called "digital dust." Invisible and often unknown to users, these data trails can be analyzed by third parties to show where users have been digitally and in real life, and what they were doing during that time.[28] Such data can be used to indirectly measure device users' health habits, such as how often they visit fast food restaurants, how often they use a gym of which they are a member, and whether they commute by car or bicycle. These types of data can be aggregated, analyzed, and repackaged for sale, often under the description of "social determinants of health."

For example, one company has created a set of health scores built on "hundreds of clinically-validated socioeconomic attributes" compiled from more than 10,000 sources of public and proprietary records.[29] These scores can predict health-related outcomes such as medication adherence and hospital readmissions, and both the data and the risk scores are marketed to payers and providers (e.g., physicians, pharmacists),[29–31] all without the consumers' awareness or informed consent. Other business models market risk scores to employers interested in engaging employees in health and wellness programs.[32]

PGHD originate from many sources and locations, and take many forms, and there are few guidelines within health care to address how they may or should be collected, managed within archives, used, re-used for other purposes, shared with other entities within and outside health care, and transmitted to others.[14,33] Many, if not most, patients and consumers have little to no awareness of just how fluid the data stream between data sources and data users may be. They may have even less understanding of whether (and if so, how) they might manage the flow of the 10,000+ sources that could have their personal data.[34] Because 61% of workers with employer-based coverage are enrolled in health plans that are completely or partially self-funded by their

employers, employers benefit from ensuring that workers understand whether and how employers and insurers could use these data, including whether employees are responding to financial incentives to participate in screening and wellness activities.[35] However, employees who would prefer not to share their sensitive PHI with their employers may not have a way to opt out of this tracking, which can result in higher health risk ratings, higher premiums, or even job loss for no apparent reason.

Although informed consent processes are intended to provide guidance for participating in clinical procedures or research, in practice such documents are often highly technical, wordy, or difficult for patients to understand, and patients may feel pressured, with little time or opportunity to review such legal agreements and ask questions.[28] Individuals commonly experience these challenges in consent forms for clinical procedures and participation in research, as well as when downloading health-related smartphone apps.[36–39] If patients agree to data sharing they do not fully understand, by the time they realize that they prefer a more restrictive approach it may be too late to "unshare" data about them.[33] Often patients must decide between the potential for services that may be valuable and the risk that data generated during those services will be used contrary to their preferences and even safety.

Facebook activities offer multiple examples of potential problems that can affect patients adversely. The social media platform has:

- Shared with third parties PHI of members of several closed support groups for people with genetic mutations that predispose them to cancer, which members believed to be private based on Facebook's terms of use.[40,41]
- Collected data directly from health apps even if the user does not have a Facebook account.[42]
- Approached hospitals about combining clinical patient data with Facebook data, de-identifying data, and providing it for research purposes.[43] Because 99.8% of Americans could be re-identified in any dataset using 15 demographic attributes,[44] it is unlikely that Facebook's proposed research data would truly be de-identified.

Although Facebook leadership has publicly called for combining social media data with medical record information to gain insights into social determinants of health through an article in the *Journal of the American Medical Association*,[45] Facebook has neither pledged an intent to protect PHI nor delineated a plan for how it can and—more importantly—*will* do so. Facebook's intent to merge social media data with medical information covered by U.S. privacy laws, with the support of medical professionals,[46] increases the possibility that information will be shared in ways the individuals do not intend and have not agreed to, even if the individuals wished to keep it confidential and/or are unaware that the information exists (e.g., insights gained via analysis using artificial intelligence).

As these examples indicate, business practices that support popular data-generating tools may not handle PGHD as individuals intend or expect, creating a need for more transparency about the flow of data.

Risks of Unintended, Unexpected, and Unconsented Data Sharing

Erosion of trust is among the most significant risks arising from the lack of privacy and security protections for data generated by individuals. If individuals do not believe that the information they are populating into mobile apps and devices and sharing within health social media groups is safe and protected, or if they see this information being easily bought and sold without their knowledge or consent, they may not use those tools or may censor their use.[47–50] This may mean they forego the benefits of use for themselves and also discourages ethical uses, such as sharing their data for research of rare diseases.

If "digital dust," often collected without an individual's knowledge (much less consent) while they are online, is unexpectedly used to make decisions about them or about subpopulations with which they identify, they may stop using Internet or online tools to search for health information for themselves or others, or to interact with others who share their health needs and interests. Their mistrust is magnified if they perceive these data to be readily available to everyone—health care providers and their business associates as a matter of course, as well as for commercial gain by third parties—except the individuals themselves. In addition, they may be categorized into subpopulations that do not accurately describe them or to which they do not regard themselves as belonging. The downstream effects of these misclassifications (e.g., received direct marketing obviously intended for members of a different group) may further erode their trust, understandably so.

Health systems and payors may lack trust in PGHD from these tools if the data are perceived to be inaccurate or less than complete (due to individual reluctance to fully utilize them, understand them, or to disclose fully and honestly) or unreliable (because data being collected are based on inferences or due to doubts about the origins of, or security protections, for this data).[51,52] Inaccurate and/or incomplete data can result in incorrect decisions by clinicians, leading to poor health outcomes in patients, as well as skewed research results, loss of reimbursement for care and/or research funding, malpractice litigation, and other undesirable outcomes for health systems, so health systems approach new technologies with caution.

Systems and payors may be reluctant to trust the outcome of algorithms whose inputs may be potentially biased as to racial and gender identities; are not transparent; or that have other potential negative outcomes that are difficult to predict or mitigate.[53,54] Conversely, they may simply trust what they believe the algorithmically analyzed data tell them and make inaccurate diagnoses, thereby setting themselves up for non-beneficial and/or dangerous or discriminatory data use by third parties, such as targeting patients for ads for products and services that may be unnecessary or even harmful.

Every data breach has implications for public trust of technology, health systems, and health research. As long as policies on collecting, storing, using, and sharing data are not transparent and consequences for misinformation and violations are not disclosed or enforced, knowledgeable consumers may be reluctant to agree to share or donate data about them.

►Fig. 1 illustrates the range of possible combinations of levels of risk disclosed and discussed by participants in the workshops. The illustration reflects the vast number of sources of data and the variations in the amount of control individuals are able to exert over their own personal health data. Individuals may experience multiple adverse effects simultaneously, as described in the accompanying vignette "How Bad Can It Get?"

Current Policy Context

The U.S. approach to health data privacy is fragmented and the most foundational policies are more than 20 years old, having been written long before the digitization of health care.[55] Subsequent policy "patches" are narrowly tailored to specific data types, such as genetic information, or organizational settings, such as care delivery or research operations. This patchwork is insufficient to protect PGHD and is ill-suited for the evolving technology landscape and scope of health data. ►Table 1 illustrates the policy patchwork and summarizes the provisions of key U.S. federal laws governing health information that are relevant to PGHD.

Despite two decades of continuous legislative and regulatory activity intended to promote the information-sharing interests of patients and clinicians, technology advances and business practices have far outpaced adjustments in federal policy,[56] resulting in unnecessary risk and frustration for everyone while still not supporting real-time access to key information. The privacy, security, and breach notification regulations under the Health Insurance Portability and Accountability Act (HIPAA) govern the use and disclosure of identifiable health information (known as protected health information)—but only when that information is held by covered entities (most health care providers and health plans) and their contractors (otherwise known as "business associates"). PHI is routinely shared outside of HIPAA's coverage, including when patients upload information into a mobile health app of their choosing. Commercial entities collecting personal information are required by federal law (the Federal Trade Commission Act or FTCA) to adopt reasonable security safeguards and uphold their commitments to consumers regarding how data are accessed, used, and shared. But notwithstanding these baseline protections, unauthorized transmission of digital data- or data leakage —occurs.[57]

New U.S. policies that require certified electronic medical records to make PHI available to consumer apps via APIs

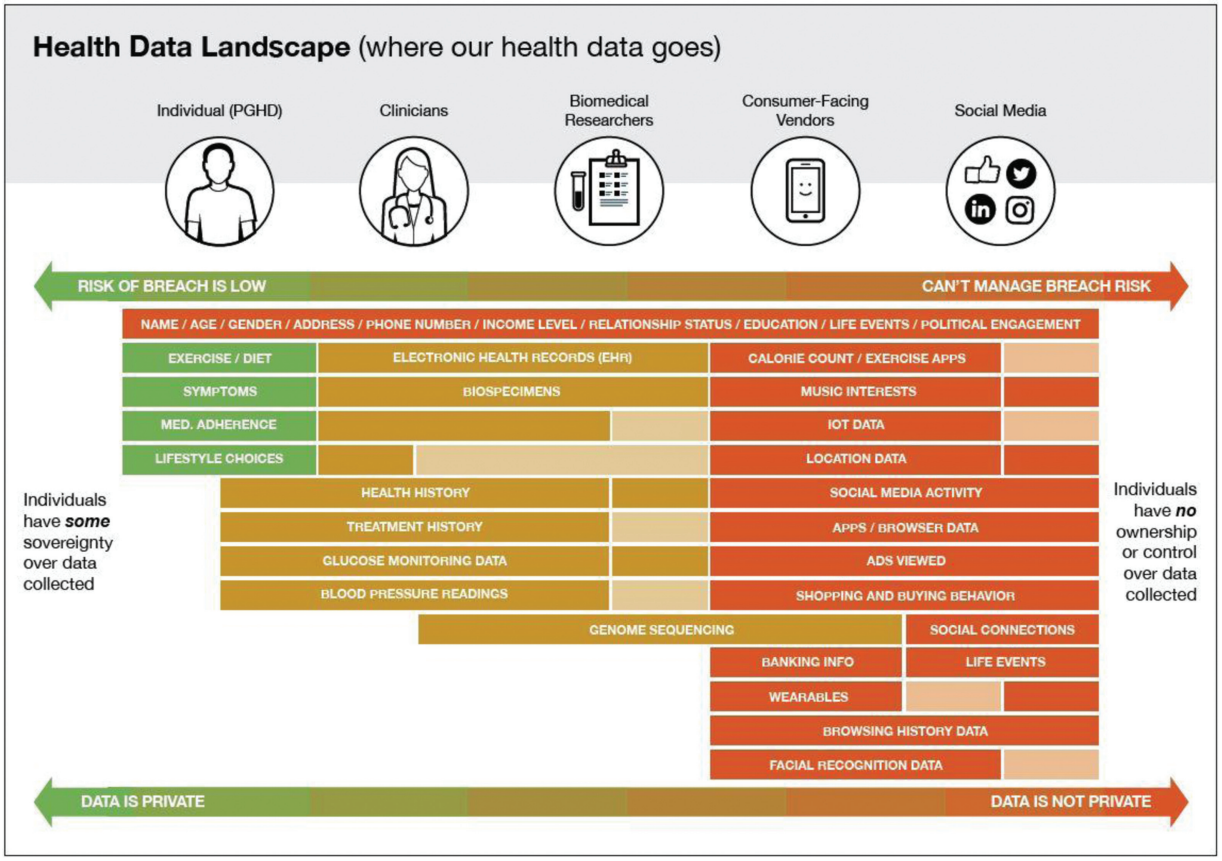

Fig. 1 *The continuum of risk for person-generated health data.* The Health Data Landscape illustrates the relative likelihood that various types of personal information (e.g., demographic, socioeconomic, health-related, financial) will be collected and/or shared without individuals' knowledge and/or permission. Figure designed by Hugo Campos for *Improving the Care Experience: A Collaborative Consensus Project.*

Table 1 Current Legal and Regulatory Landscape: Privacy Protections for PGHD used for shared decision-making. This table summarizes key federal legislation and regulations in the U.S. related to patient/individual data privacy and PGHD for shared decision-making. The table clarifies patients' rights with regard to data access and control; the obligations of entities covered by the law (for example, under HIPAA Covered Entity [CEs], Business Associates [BAs], and health care researchers); coverage of consumer-facing technology companies that manages or uses patient/individual data (if any); and prohibitions (if any) that limit how patient/individual data may be used.

	Rights	Obligations	Prohibitions and limitations
HIPAA Privacy, Security, and Breach Notification Rules	• Grants patients the right to: • Access their protected health information (PHI) maintained by or for a CE. • Access laboratory test reports from Clinical Laboratory Improvement Amendments (CLIA)-certified or CLIA-exempt laboratories. • Transmit their PHI to a 3rd party. • Receive an accounting of parties who have received their PHI for purposes other than treatment, payment or health care operations (Accounting of Disclosures). • Decide whether to share their PHI for purposes of research through an authorization or informed consent (unless the authorization requirement is waived by an institutional review board [IRB] or Privacy Board). • Control whether and how their PHI is used and disclosed for marketing purposes. • Control whether their PHI can be sold. • Request amendments to their PHI. • Request restrictions on how their PHI can be used and disclosed (up to the entity on whether to honor, except as noted below). Demand their PHI not be disclosed to payers if patients pay out of pocket in full for services. • Be notified of breaches of their health information by a covered entity.	Requires CEs and BAs to protect PHI by maintaining reasonable: • Administrative safeguards • Physical safeguards • Technical safeguards. Requires CEs to: • Garner a patient's prior written authorization to use or disclose PHI for any purpose not expressly permitted by the regulations—for example, sales of PHI and uses or disclosures of PHI for marketing purposes. • Assure in writing (e.g., via contract) that its BAs will appropriately safeguard the protected health information it receives or creates on behalf of the CE. • Notify individuals (and the federal government) in the event of breaches of PHI. Requires researchers who work for CEs to obtain an individual's authorization for research containing non-de-identified PHI or a waiver of authorization is granted by an IRB or Privacy Board.	All things not permitted by HIPAA may be done with the authorization of the individual through a HIPAA-compliant authorization. Consumer-based technology companies have no obligations with regard to data management and/or use practices in HIPAA.
HITECH Act	Grants patients the right to be notified of a breach of their PHI by a personal health record vendor (e.g., an mHealth app).	Requires personal health record vendors to notify individuals and the Federal Trade Commission of breaches of their identifiable information.	None
21st Century Cures Act	Extends the rights of individuals to access their complete medical record and all electronic health information (EHI) held by a provider or a health information network through prohibitions on information blocking. Provides patients with the right to access key aspects of their health information through the app of their choice via application programming interfaces (APIs) in provider electronic medical records (effective in 2022–2023).	Requires providers and health information networks to provide patients (upon request) with key aspects of their health information. More information to be provided to patients (or an app chosen by the patient) via APIs by 2022.	Applies only to providers, certified electronic health record vendors, and health information networks. Applies only to information in the U.S. Core Data Set for Interoperability, which is not all information the patient has the right to under HIPAA.
Part 2	Grants patients' rights to consent prior to disclosures of their identifiable health information, in most circumstances (including for treatment purposes).	Requires individual consent to share for most purposes, including treatment. Entities covered by HIPAA and Part 2 may disclose data for research purposes consistent with HIPAA (for example, with authorization, with a waiver of authorization, or under broad consent provisions).	Prohibits law enforcement access to identifiable data without a court order. Applies only to federally supported substance abuse treatment facilities and programs (although identifiable data from a Part 2-covered program continues to be covered by Part 2 even if it is lawfully disclosed to another entity). No express individual rights to access data. No consent required to share data for treatment purposes in a "bona fide" medical or national emergency. *Of note: the Coronavirus Aid, Relief, and Economic Security (CARES) Act made some changes to these regulations

(*Continued*)

Table 1 (*Continued*)

	Rights	Obligations	Prohibitions and limitations
Common Rule	Grants patients the right to choose whether or not to allow their identifiable health information to be accessed for research (either specific research projects or broadly defined) when research is performed by an entity subject to the Rule.	Requires researchers covered by the Rule to: • Receive approval from an IRB or Privacy Board prior to conducting a study that will use PHI. • Either seek consent or obtain waiver of consent from an Institutional Review Board prior to using identifiable health information for research purposes.	Does not apply to data that are not identifiable to researchers (not considered to be human subjects research).
FTC Act	None	None	Applies to most consumer technologies. Prohibits deceptive or unfair acts or practices in or affecting commerce, including those relating to privacy and data security, and those involving false or misleading claims about apps' handling of personal data, safety, or performance.
Genetic Information Nondiscrimination Act	Individuals have a right to pursue private litigation if they feel they have been discriminated against in employment. Health insurance discrimination on the basis of genetic information may be a violation of the Affordable Care Act or other civil rights laws.		Prohibits health insurers from: • Using genetic information to make eligibility, coverage, underwriting or premium-setting decisions. • Requesting or requiring individuals or their family members to undergo genetic testing or to provide genetic information. • Using genetic information to make any decisions about health insurance benefits, eligibility for benefits, or the calculation of premiums under a health plan. Prohibits employers from using genetic information in employment decisions such as hiring, firing, promotions, pay, and job assignments Prohibits employers or other CEs (employment agencies, labor organizations, joint labor-management training programs, and apprenticeship programs) from requiring or requesting genetic information and/or genetic tests as a condition of employment.

further complicate the landscape, given the interest such vendors may have in acquiring and using PHI for commercial purposes. In examining the increasing reliance on patient-facing APIs to promote patient access to their clinical information, a U.S. Office of the National Coordinator for Health Information Technology Task Force noted that an app may need to comply with several federal laws, including HIPAA (if the app is being offered by a covered entity or business associate), the Federal Trade Commission Act (FTC Act), and the FTC's Health Breach Notification Rule, among others.[58] Recent guidance from the U.S. Food and Drug Administration also attempts to clarify what apps are regulated medical devices that require FDA review and approval for safety and efficacy (FDA does not regulate the privacy of information collected by apps).[59] But not withstanding that some laws do apply to these apps, they do not provide the comprehensive framework for privacy and security that may be needed to build and maintain consumer trust in these tools.[60]

Although the focus of this article is to assure protections for data that fall outside of the coverage of HIPAA, HIPAA itself is not without its flaws. Health care organizations seek to comply with state and federal statutes, but struggle to do so despite the availability of detailed guidance from regulators because of differences in legal interpretations.[61–63] As a result, organizations often are reluctant to release any patient information over fear of violating the law and potentially incurring financial penalties.[64] Information blocking, a set of practices undertaken by vendors and providers that restrict access to patient information, has been characterized as a revenue enhancement strategy.[65] A 2016 study of the top 20 hospitals rated by *U.S. News and World Report* found many were not meeting federal requirements for medical records formats and timeliness of processing.[66] Also, notwithstanding clear mandates in HIPAA since 2001 to provide patients with easy access to their health information, patients still struggle to get copies of their health data.

However, change may be on the horizon. The HHS Office for Civil Rights—which enforces HIPAA—announced in February 2019 that it would be launching a new HIPAA Right of Access enforcement initiative. OCR reached its first settlement in this new initiative in early September 2019,[67] which may be a harbinger of more active federal oversight and enforcement

on behalf of consumer access to data. Another approach is a public scorecard recently implemented by Ciitizen, in which health care provider organizations receive scores on their responses to actual patient requests for their own records.[68] Regulations penalizing "information blocking," which were issued by the HHS Office of the National Coordinator pursuant to the 21st Century Cures Act, will go into effect as of April 2021,[69] and provider electronic medical record technology will be equipped with patient-facing APIs no later than mid-2022. These initiatives will spur greater access by patients to comprehensive clinical data—but also increase the pressure on policymakers to assure privacy and security protections for data that fall outside of HIPAA protections.

Building a Better Future: Policy Recommendations

A new policy framework is needed to facilitate a data-rich environment that leads to better SDM, where individuals trust that they can actively use online and mobile tools to collect, use, and share PGHD, both in pursuit of their own individual health and wellness goals as well as to improve the health and wellness of others. The following recommendations originated as policy priorities in workshop discussions and were refined in subsequent discussions by the coauthors. They are consensus-based, consumer-driven, and outline some key best practices for the collection, use, and sharing of PGHD not covered under HIPAA, except as noted to support HIPAA compliance.

Recommendation 1: Policymakers should assure privacy, security, and ethical protections for PGHD (all person-generated data used for health and wellness purposes) are in place, regardless of which entity is holding the data.

- As highlighted in ►Table 1, data used for health and wellness purposes are not protected in all settings.
- Policymakers should act to fill gaps in current protections and, for existing laws, regulatory agencies should enact and robustly enforce regulations (including penalties) of sufficient weight to promote compliance and enable a trusted environment for the collection, use, and sharing of PGHD. Additional action is needed by Congress to make this possible.
- Protections for PGHD should be sufficiently comprehensive to, at a minimum, facilitate recommendations 2 to 5.

Recommendation 2: Individuals must be able to access PGHD data about them electronically, promptly after it is generated ("real-time"), at their convenience using their preferred method(s).

- Policymakers should ensure that individuals are able to identify, access, and manage their PGHD—including the ability to request correction of inaccurate information—in a timely manner and at a reasonable cost. Without a guarantee of access to their data upon request supported by appropriate regulation, individuals have no reason to trust data-gathering institutions, whether such organizations are health care-based or commercial.
- This access should include all PGHD, including data covered by HIPAA (such as that generated through clinical care and payment encounters) as well as through commercial transactions, such as purchasing over-the-counter medications and visiting a gym or a website.

Recommendation 3: Collection of PGHD should include a robust, consistent, and transparent process for ensuring that informed consent occurs whenever and wherever the potential for data sharing arises.

- Any agreement, contract, or terms of service offered to an individual should include a straightforward delineation of the individual's rights regarding their access to data about them as well as how those data are stored and may be used or shared by companies, researchers, and organizations. Agreements also should clearly state the costs that individuals must bear, if any.
- To the extent feasible, this process should include mechanisms (e.g., opt-in approaches) through which individuals can identify potential data uses they are consenting to when data about them are collected and restrict access to this data (in terms of use or in terms of duration) without limiting its use for either the individual or the public good.
- This informed consent process must include information on how individuals can contact the organization or company storing data about them and a process by which they can change or update their ongoing consent.
- Individuals should be able to update their preferences at any time, including the right to withdraw access by entities with which they have previously shared their information.
- Individuals should be able to choose the tool(s) they use to share data about them.

Recommendation 4: Individuals should be able to ensure that researchers can use data about them for meaningful medical research.

- Individuals often wish to contribute data about them for medical research, and they should be able to donate this data, as well as require others who hold this data to contribute it for research purposes (including when those data are held by entities covered by HIPAA). After consent has been given, researchers should cover any costs associated with PGHD use.
- Policies and regulations in the PGHD context should ensure that individuals are aware of the past and present uses of data about them for research purposes and consent to future data use. The circumstances under which the data could be used for research, how long the data can be retained by research organizations, and the circumstances under which individuals (and their families) could later rescind the continued use of data about them for research should be clearly disclosed.

Recommendation 5: Uses of PGHD must be ethical and fair to individuals and populations.

- Non-health-related uses of PGHD (e.g., for marketing of non-health-related products such as cigarettes or alcohol)

that could cause harm to individuals, subpopulations, or populations (e.g., law enforcement access without a warrant or insurer use to redline individuals or populations out of benefits) should be prohibited.
- Tracking of data about individuals, vulnerable groups (e.g., elderly persons, people with disabilities), and historically targeted groups (e.g., people of color) based on data collected for specific purposes beneficial to the public (such as public health) should be limited to health-related uses that benefit individuals, subpopulations, and/or populations.
- Ongoing, objective, ethical review of initiatives focused on analysis of PGHD should be undertaken to ensure that such analytics are conducted in a way that promotes learning by individuals, care providers, and health care systems and minimizes harm to individuals and populations. Review bodies that include the full range of affected stakeholders—including patients, caregivers, consumers, and community representatives—can promote trust by ensuring transparency around ongoing work and forcing robust public discussion of proposed new efforts.

Conclusion

From the perspective of individuals, there are many opportunities to improve health data management policy and its implementation across health care organizations, health information exchanges, and consumer-facing health management tools. With a SDM process, PGHD have the potential to inform which treatment(s) patients choose and how they are given, decisions that confer power to shape the future directions and goals of research.

In addition, the ability to re-use clinical data offers significant opportunities for the advancement of practice, the reduction of health disparities, and the promotion of health equity—*if* we develop and implement at scale improved processes supported by realistic, appropriate, and transparent policies. Health policies that more closely align to individuals' needs and goals, as well as their expectations with regard to consent, data sharing, and transparency about use of data about them, will encourage SDM and facilitate more positive experiences for individuals, clinicians, and care teams alike.

How Bad Can It Get?

John, a 36-year-old man with a knee injury and diagnosed anxiety, works at a large corporation that self-insures. His employer offers a wellness program that uses algorithms to identify the best ways to incentivize employee self-care.

John's credit card transaction data reflect regular visits to fast food restaurants and insurance claim-eligible purchases revealing his anxiety diagnosis. Through these and other data sources, he is invited to participate in counseling for healthy eating offered via his employer's wellness program. He declines, because he is concerned about what his employer will do with information about where he eats and that he has anxiety. It already makes him uncomfortable that he gets served ads for anti-anxiety medications on his phone and his computer. One time he handed his phone to a friend to show her his vacation photos, and one of those ads popped up. He also doesn't think it's any of his employer's business where he eats. Because he declined the program to try to keep his information more private, his monthly health insurance premium increases $100/month the following year.

When John's knee pain worsens, he is referred for an MRI. At the follow-up appointment, John's orthopedist tells him that he has an elevated surgical risk score created from clinical and "social factors." John is unsure what "social factors" are but decides not to pursue surgery as a result.

Still dealing with his unresolved and painful knee condition, several months later John receives a phone call from a debt collector for an unpaid medical bill. He logs into his insurance Web portal and finds claims from doctors he did not visit. He assumes it's a mistake and calls the clinic he visited for his knee pain. John explains his situation, and it becomes clear that he is a victim of medical identity fraud. When he requests a copy of his own medical record to correct it, the clinic refuses access.[72] The customer service representative wrongly tells John that the clinic must preserve the identity thief's right to privacy, even though the medical record is John's. Shocked and confused, he declines to pursue the matter.

Six months later John receives a notice that a local radiology clinic had a breach of patient protected health information (PHI) when scans were made available on the Internet,[73] and that he is among those whose PHI was exposed. He realizes that his knee MRI led to the theft of his medical identity, and that he is now among the 25% of Americans who have had health information stolen.[74]

After 2 years, hundreds of hours, and more than $10,000 in legal fees and incorrect medical bills, John continues working to repair the damage to his identity and his health.[75] He continues to pay higher insurance premiums because of his concerns about the data collection required for his participation in the wellness program. His knee also still continues to bother him.

Clinical Relevance Statement

The evolution of patient–clinician relations from paternalistic to more egalitarian engagement has resulted in broader use of SDM as the basis for treatment planning and created a need for re-assessment of factors influencing adoption of SDM. At the same time, the increasing availability and usability of PGHD are opening up new opportunities for care management and treatment monitoring for clinicians

and patients engaging in SDM. This article provides policy recommendations for removing barriers to the collection, use, and sharing of PGHD for health care management and research.

Note

This work is one of four papers co-authored by participants in a collaborative consensus project to develop a framework for using person-generated health data in shared decision-making. Each writing team included at least one consumer or caregiver representative along with other research, policy, and technology experts, and a user experience designer. The work was overseen by a diverse multisector advisory group co-chaired by Hugo Campos and Katherine Kim, with Jeffrey Corkran, Patricia Franklin, Sarah Greene, Megan O'Boyle, and Carolyn Petersen. Advice and consultation with Dana Lewis, Liz Salmi, and John Wilbanks and assistance and support from Lauren Adams and Tamara Infante are gratefully acknowledged. All statements in this report, including its findings and conclusions, are solely those of the authors and do not necessarily reflect the views of the Patient-Centered Outcomes Research Institute (PCORI) or its Board of Governors.

Authors' Contributions

M.E., H.C., and C.P. planned the workshop. Manuscript was approved by C.P. All the authors developed the recommendations and drafted the manuscript.

Protection of Human and Animal Subjects

No human subjects were involved in this project and institutional review board approval was not required.

Funding

Financial support for this work was provided by a Eugene P. Washington PCORI engagement award to Margo Edmunds at AcademyHealth.

Conflict of Interest

D.M. reports other relevant activities from Ciitizen Corporation, personal fees from All of U.S. Research Program IRB, personal fees from Verily's Project Baseline Advisory Board, and other relevant activities from Datavant, outside the submitted work. J.R.L.S. was an American Medical Informatics Association employee during the period when this manuscript was being developed; his views are his own and not those of HHS or the Office of the National Coordinator for Health IT. The remaining authors report no conflict of interest.

References

1 Beach MC, Sugarman J. Realizing shared decision-making in practice. JAMA 2019;322(09):811–812
2 Elwyn G, Frosch D, Thomson R, et al. Shared decision making: a model for clinical practice. J Gen Intern Med 2012;27(10):1361–1367
3 Office of the National Coordinator for Health Information Technology. Shared decision-making fact sheet; 2013. Accessed October 9, 2019 at https://www.healthit.gov/sites/default/files/nlc_shared_decision_making_fact_sheet.pdf
4 Bardach E. A Practical Guide for Policy Analysis: the Eightfold Path to More Effective Problem Solving. New York: Chatham House Publishers; 2000
5 Engelman A, Case B, Meeks L, Fetters MD. Conducting health policy analysis in primary care research: turning clinical ideas into action. Fam Med Community Health 2019;7(02):e000076
6 Davis S, Roudsari A, Raworth R, Courtney KL, MacKay L. Shared decision-making using personal health record technology: a scoping review at the crossroads. J Am Med Inform Assoc 2017;24(04):857–866
7 Edmunds M. Promoting consumer engagement in health and healthcare. InEdmunds M, Hass C, Holve E, eds. Consumer Informatics and Digital Health: Solutions for Health and Healthcare. Berlin, Germany: Springer; 2019:3–24
8 Lai AM, Hsueh PS, Choi YK, Austin RR. Present and future trends in consumer health informatics and patient-generated health data. Yearb Med Inform 2017;26(01):152–159
9 Smith TG, Dunn ME, Levin KY, et al. Cancer survivor perspectives on sharing patient-generated health data with central cancer registries. Qual Life Res 2019;28(11):2957–2967
10 Hartzler AL, Taylor MN, Park A, et al. Leveraging cues from person-generated health data for peer matching in online communities. J Am Med Inform Assoc 2016;23(03):496–507
11 Petersen C. Through patients' eyes: regulation, technology, privacy, and the future. Yearb Med Inform 2018;27(01):10–15
12 Arigo D, Pagoto S, Carter-Harris L, Lillie SE, Nebeker C. Using social media for health research: methodological and ethical considerations for recruitment and intervention delivery. Digit Health 2018;4:2055207618771757
13 Terrasse M, Gorin M, Sisti D. Social media, e-health, and medical ethics. Hastings Cent Rep 2019;49(01):24–33
14 Petersen C, DeMuro P. Legal and regulatory considerations associated with use of patient-generated health data from social media and mobile health (mHealth) devices. Appl Clin Inform 2015;6(01):16–26
15 Pagoto S, Nebeker C. How scientists can take the lead in establishing ethical practices for social media research. J Am Med Inform Assoc 2019;26(04):311–313
16 Mennemeyer ST, Menachemi N, Rahurkar S, Ford EW. Impact of the HITECH Act on physicians' adoption of electronic health records. J Am Med Inform Assoc 2016;23(02):375–379
17 Health IT and Patient Safety: Building Safer Systems for Better Care. Committee on Patient Safety and Health Information Technology; Institute of Medicine. Washington, DC: National Academies Press (US); 2011
18 DesRoches CM, Bell SK, Dong Z, et al. Patients managing medications and reading their visit notes: a survey of OpenNotes participants. Ann Intern Med 2019;171(01):69–71
19 OpenNotes. More Than 40 Million Patients Can Access Their Clinicians' Visit Notes Via Secure Portals at 200 Health Systems. Accessed September 22, 2019 at: https://www.opennotes.org/news/more-than-40-million-patients-can-access-their-clinicians-visit-notes-via-secure-portals-at-200-health-systems/
20 Gerard M, Fossa A, Folcarelli PH, Walker J, Bell SK. What patients value about reading visit notes: a qualitative inquiry of patient experiences with their health information. J Med Internet Res 2017;19(07):e237
21 Blumenthal D, Abrams MK. Ready or not, we live in an age of health information transparency. Ann Intern Med 2019;171(01):64–65
22 Vodicka E, Mejilla R, Leveille SG, et al. Online access to doctors' notes: patient concerns about privacy. J Med Internet Res 2013;15(09):e208

23 Wright E, Darer J, Tang X, et al. Sharing physician notes through an electronic portal is associated with improved medication adherence: quasi-experimental study. J Med Internet Res 2015;17(10): e226
24 Edmunds M, Peddicord D, Frisse ME. 2016. The evolution of health information technology policy in the United States. InBall M, Weaver C, Kiel C, eds. Healthcare Information Management Systems: Cases, Strategies, and Solutions. Cham, Switzerland: Springer; 2016
25 Pifer R. Q&A: ONC chief Don Rucker on bringing the app economy into healthcare. HealthcareDive. Accessed September 15, 2019 at: https://www.healthcaredive.com/news/qa-onc-chief-don-rucker-on-bringing-the-app-economy-into-healthcare/561436/
26 Singhal S, Carlton S. The era of exponential improvement in healthcare? Accessed September 26, 2019 at: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-era-of-exponential-improvement-in-healthcare
27 Kim KK, Jalil S, Ngo V. Improving Self-Management and Care Coordination with Person-Generated Health Data and Mobile Health. Consumer Informatics and Digital Health: Solutions for Health and Healthcare. Berlin, Germany: Springer; 2019
28 Wilbanks J. Ethical issues in consumer informatics and online content. InEdmunds M, Hass C, Holve E, eds. Consumer Informatics and Digital Health: Solutions for Health and Healthcare. Berlin, Germany: Springer; 2019
29 LexisNexis. Socioeconomic health score. Accessed September 15, 2019 at: https://risk.lexisnexis.com/products/socioeconomic-health-score
30 LexisNexis. Socioeconomic health attributes for providers. Accessed September 15, 2019 at: https://risk.lexisnexis.com/products/socioeconomic-health-attributes
31 Allen M. Health insurers are vacuuming up details about you—and it could raise your rates. ProPublica. Accessed September 14, 2019 at: https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates
32 Welltok. Total wellbeing solution for employers. Accessed on September 15, 2019 at: http://www.welltok.com/employers/
33 Petersen C. User-focused data sharing agreements: a foundation for the genomic future. JAMIA Open 2019;2(04):402–406
34 Haug CJ. Whose data are they anyway? Can a patient perspective advance the data-sharing debate?. N Engl J Med 2017;376(23): 2203–2205
35 Kaiser Family Foundation. Self-Funded Plans: 2018 Employer Health Benefits Survey. Accessed on September 14, 2019 at: https://www.kff.org/report-section/2018-employer-health-benefits-survey-summary-of-findings/
36 Eltorai AE, Naqvi SS, Ghanian S, et al. Readability of invasive procedure consent forms. Clin Transl Sci 2015;8(06):830–833
37 Perrenoud B, Velonaki VS, Bodenmann P, Ramelet AS. The effectiveness of health literacy interventions on the informed consent process of health care users: a systematic review protocol. JBI Database Syst Rev Implement Reports 2015;13(10):82–94
38 Foe G, Larson EL. Reading level and comprehension of research consent forms: an integrative review. J Empir Res Hum Res Ethics 2016;11(01):31–46
39 Fowler LR, Gillard C, Morain SR. Readability and accessibility of terms of service and privacy policies for menstruation-tracking smartphone applications. Health Promot Pract 2020;21(05): 679–683
40 Downing A. How a patient advocate discovered a massive security problem with closed groups on Facebook and became a white hat hacker. Accessed September 1, 2019 at: https://bravebosom.org/2018/07/04/sicgrl/
41 Federal Trade Commission. United States of America v. Facebook, Inc., a corporation. Accessed September 1, 2019 at: https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc
42 Schechner S, Secada M. You give apps sensitive personal information. Then they tell Facebook. The Wall Street Journal. Accessed September 15, 2019 at: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636
43 Farr C. Facebook sent a doctor on a secret mission to ask hospitals to share patient data. CBNC. Accessed September 15, 2019 at: https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html
44 Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 2019;10(01):3069
45 Abnousi F, Rumsfeld JS, Krumholz HM. Social determinants of health in the digital age: determining the source code for nurture. JAMA 2019;321(03):247–248
46 Estabrooks PA, Boyle M, Emmons KM, et al. Harmonized patient-reported data elements in the electronic health record: supporting meaningful use by primary care action on health behaviors and key psychosocial factors. J Am Med Inform Assoc 2012;19 (04):575–582
47 Hewitt C, Lloyd KC, Tariq S, et al. Patient-generated data in the management of HIV: a scoping review. BMJ Open 2021;11(05): e046393
48 Iott BE, Campos-Castillo C, Anthony DL. Trust and privacy: how patient trust in providers is related to privacy behaviors and attitudes. AMIA Annu Symp Proc 2020;2019:487–493
49 Peek ME, Gorawara-Bhat R, Quinn MT, Odoms-Young A, Wilson SC, Chin MH. Patient trust in physicians and shared decision-making among African-Americans with diabetes. Health Commun 2013;28(06):616–623
50 Ruotsalainen P, Blobel B. Health information systems in the digital health ecosystem—problems and solutions for ethics, trust and privacy. Int J Environ Res Public Health 2020;17(09):3006
51 Bietz MJ, Bloss CS, Calvert S, et al. Opportunities and challenges in the use of personal health data for health research. J Am Med Inform Assoc 2016;23(e1):e42–e48
52 Zhu H, Colgan J, Reddy M, Choe EK. Sharing patient-generated data in clinical practices: an interview study. AMIA Annu Symp Proc 2017;2016:1303–1312
53 Isakadze N, Martin SS. How useful is the smartwatch ECG? Trends Cardiovasc Med 2019
54 Rajakariar K, Koshy AN, Sajeev JK, Nair S, Roberts L, Teh AW. Accuracy of a smartwatch based single-lead electrocardiogram device in detection of atrial fibrillation. Heart 2020;106(09): 665–670
55 Bari L, O'Neill DP. Rethinking patient privacy in the era of digital health. Accessed May 23, 2021 at: https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/
56 Rosenbloom ST, Smith JRL, Bowen R, Burns J, Riplinger L, Payne TH. Updating HIPAA for the electronic medical record era. J Am Med Inform Assoc 2019;26(10):1115–1119
57 Leom MD, Choo KR, Hunt R. Remote wiping and secure deletion on mobile devices: a review. J Forensic Sci 2016;61(06):1473–1492
58 Office of the National Coordinator for Health Information Technology Application Programming Interface (API) Task Force. API Task Force Recommendations. Accessed September 15, 2019 at: https://www.healthit.gov/sites/default/files/facas/SingleSourceofTruth-APITFRecommendations.pdf
59 Food and Drug Administration. Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. Accessed September 15, 2019 at: https://www.fda.gov/media/80958/download
60 McGraw D, Petersen C. From commercialization to accountability: responsible health data collection, use, and disclosure for the 21st century. Appl Clin Inform 2020;11(02):366–373
61 Office of the National Coordinator for Health Information Technology. Permitted Uses and Disclosures: Exchange for Health Care Operations. Accessed September 15, 2019 at: https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf

62 Office of the National Coordinator for Health Information Technology. Permitted Uses and Disclosures: Exchange for Treatment. Accessed September 15, 2019 at: https://www.healthit.gov/sites/default/files/exchange_treatment.pdf
63 Office of the National Coordinator for Health Information Technology. Permitted Uses and Disclosures: Exchange for Public Health Activities. Accessed September 15, 2019 at: https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf
64 Office of the National Coordinator for Health Information Technology. 2016 Report to Congress on Health IT Progress: Examining the HITECH Era and the Future of Health IT. Accessed September 15, 2019 at: https://dashboard.healthit.gov/report-to-congress/2016-report-congress-examining-hitech-era-future-health-information-technology.php#executive-summary
65 Adler-Milstein J, Pfeifer E. Information blocking: is it occurring and what policy strategies can address it? Milbank Q 2017;95(01):117–135
66 Lye CT, Forman HP, Gao R, et al. Assessment of US hospital compliance with regulations for patients' requests for medical records. JAMA Netw Open 2018;1(06):e183014
67 Health and Human Services. OCR Settles First Case in HIPAA Right of Access Initiative. Accessed September 9, 2019 at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bayfront/index.html
68 Ciitizen. The Patient Record Scorecard: What It Is and Why We Did It. Accessed September 29, 2019 at: https://www.ciitizen.com/the-patient-record-scorecard-what-is-it-and-why-we-did-it/
69 Office of the National Coordinator for Health Information Technology. ONC Interim Final Rule. Accessed May 23, 2021 at: https://www.healthit.gov/cures/sites/default/files/cures/2020-10/IFC_FactSheet_Information_Blocking.pdf
70 Office of the National Coordinator for Health Information Technology. Patient-Generated Health Data. March 2014. Accessed September 18, 2019 at: https://www.healthit.gov/sites/default/files/patient_generated_data_factsheet.pdf
71 Elwyn G, Edwards A, Kinnersley P, Grol R. Shared decision making and the concept of equipoise: the competences of involving patients in healthcare choices. Br J Gen Pract 2000;50(460):892–899
72 Federal Trade Commission. What To Do Right Away. Accessed September 15, 2019 at: https://www.identitytheft.gov/Steps
73 Gillum J, Kao J, Larson J. Millions of American's Medical images and data are available on the internet. Anyone can take a peek. ProPublica. Accessed September 17, 2019 at: https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet
74 Accenture. One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals. Accessed on September 16, 2019 at: https://newsroom.accenture.com/subjects/technology/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm
75 Ponemon Institute. Fifth Annual Study on Medical Identity Theft. Accessed September 18, 2019 at: http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_-Theft_Study1.pdf