

# Examining Trust and Consent Models for Patient-Generated Health Data-sharing and Incentives

Brian Thoms<sup>1</sup>, Nathan Botts<sup>2</sup>, Evren Eryilmaz<sup>3</sup>

<sup>1</sup>California State University, Channel Islands, Westat<sup>2</sup>, <sup>3</sup>California State University, Sacramento

Brian.Thoms@csuci.edu, NathanBotts@westat.com, Evren.Eryilmaz@csus.edu

## Abstract

*This research explores mitigating factors that influence personal health information sharing as it relates to the adoption of personal health information systems (PHIS). We examine the willingness of online users to share specific types of health data, their general concerns about sharing their health data, and what incentives might exist to motivate health data-sharing in the future. Findings across 336 survey respondents identify an overall sense of concern towards online data-sharing and privacy policies, and yet a willingness to share information, including personal health data, and the potential for health incentives to affect their willingness to share various types of health data. The implications of this research will play an important role as organizations and individuals increasingly adopt personal health information systems. This research also addresses the need for established guidelines and frameworks that address patient privacy as more data is captured and stored within cloud computing environments.*

**Keywords:** Consent Models, Data Sharing, Trust, Patient Generated Health Data, Patient Incentives.

## 1. Introduction

Research in 2009 identified a direct correlation to concerns for information privacy and the adoption of health information technology (HIT) [1]. In 2023, a Pew Research Study showed that concerns for information privacy persist, with individuals worried about how companies (81%) and government (71%) are using their personal data [2]. Today, users are continually asked to agree to system-mandated Terms of Service (ToS) that specify how an organization might obtain and interact with its content. In fact, privacy policies are pervasive across websites, mobile apps, and smart devices and form de facto disclosure agreements for how an organization may collect, use, and transfer your data. Moreover, these policies are continually modified even after a user's initial acceptance. Related studies have identified that a majority of Americans are asked to consent to privacy policies at least monthly [3]. Consequently, as systems continue to become tightly integrated into our daily lives, perceptions of these policies, particularly across vulnerable populations, must be continually revisited, especially as they relate to highly sensitive areas within HIT. Data collected across distributed HIT environments can be utilized to

optimize patient treatments, but this can only be done through the proper consent of HIT users [4]. This imposes new questions as to how individuals can effectively manage the consent they provide for the types of information they share and with whom they share it.

This research investigates the often-unconsidered consent many users provide across the broader spectrum of information systems, with a focus on personal health information and the willingness of online consumers to share access to their health data and the potential benefits of doing so. Further explored are the motivations individuals have for sharing personal data, the compromises they make, and their expectations of their privacy rights once the submit button is clicked. We also explore the role incentives can play for users when it comes to data sharing. Initial findings discovered that while participants were less likely to share sensitive health-related data, they would generally be willing to do so if adequately incentivized, even if they do not entirely trust data-sharing policies.

## 2. Background

### 2.1 Patient-Generated Health Data

Personal health data plays a crucial role in improving individual health outcomes, advancing medical research, and enhancing healthcare delivery at both the individual and population levels. Yet the potential for over-sharing and its impact is of increasing concern across the domain of personal health information systems (PHIS), which can include technologies such as personal health records (both patient-owned and health provider-owned), health applications (apps), and personal medical devices.

Laws such as the 21st Century Cures Act, which includes the Patient Right to Access clause, foster even further opportunities for growth in the PHIS industry [5]. As personal health informatics evolves, individuals have begun taking a more active role in managing and reporting their health activities through online applications, a practice more commonly referred to as "patient-generated health data" (PGHD) [6]. PGHD comes from an ever-increasing number of sources, including personal health records (PHR), Internet of Things (IoT) devices (e.g., glucometers), and fitness apps that track heart rate, stress, and sleep (e.g., FitBit).

Additionally, application programming interfaces (APIs) aimed at capturing PGHD, such as Apple HealthKit, can adopt data exchange standards such as HL7® Fast Healthcare Interoperability Resources (FHIR®), which can seamlessly integrate PGHD into a user's electronic health record [7]. Yet, managing consent across these systems becomes increasingly challenging, even as end-user benefits of HIT adoption can lead to better health outcomes. As a result, organizations aim to adopt incentive models to better attract users [8].

While individual ownership of one's personal health information can be seen as a positive step toward better health, caveats exist, especially when individuals utilize third-party applications to help manage sensitive health information. In many of these cases, individuals adopt shared models of personal health information ownership, where individuals are not only consumers of their electronic health records from respective healthcare organizations but are also producers of new health data based on daily health behaviors. Consequently, such relationships raise new issues of privacy and consent, especially as it relates to the added value of PGHD and its role within patient-centered and shared decision-making models of care.

## 2.2 Health Data Privacy Policies

In the U.S., considerable legal constraints exist in the form of the Health Information Portability and Privacy Act (HIPAA) that determine when patient data can be transferred and the consent directives that need to be in place before that data can be shared [9]. Efforts such as the Data Segmentation for Privacy (DS4P) project, promoted by organizations such as the Substance Abuse and Mental Health Services Administration (SAMHSA), have sought to systematically ensure that protected health data is not exchanged based on the types of data found in the health record and according to the consent policies dictated at the federal, state and personal level [10]. The U.S. Office of the National Coordinator (ONC) has established guidance on Meaningful Consent and the consent options that should be established prior to Health Information Exchange (HIE) events [11].

However, many of these policies cover only a few modern health technologies like mobile health apps, online health searches, fitness devices, and wearables that are being used outside of HIPAA and related protections for covered entities [12, 13]. These technologies often share or sell data based on the ToS, Privacy Policies, and End User License Agreements (EULA) that consumers agree to without fully understanding. Consumers may expect privacy similar to doctor-patient interactions, but many healthcare websites share user data, including geolocation and demographics, with third parties for profiling, ad-targeting, or other purposes. This data-sharing not only raises privacy concerns but also poses security threats.

## 2.3 Consent to Share

The act of consent refers to the personal action that manages and dictates the degree of privacy and security assigned to one's health information as it is shared across systems. Within medical domains of study, although consent more formally refers to "informed consent," consent can also describe many informal decisions as well. Thus, consent can be perceived as a form of self-management or self-efficacy in which an individual feels confident in their or another entity's ability to correctly act upon the behavior necessary to reach their health goals [14]. The behavioral and psychological aspects of consent and control can also play a strong role in the onset and ability to effectively apply therapy for many health conditions [15].

Consent within the domain of HIEs refers to the informed agreement of allowing parts or the whole of one's personal health information to be shared so that it can be used for various purposes. Such repurposing of health information provides many benefits, such as increased continuity between different care providers for a patient, clinical trials, re-use for health or market-related research, or re-use to inform the greater state of public health. Consent decisions pertain to the sharing and accessing of a patient's health information through some level of HIE for treatment, payment, and healthcare operations. Patients can determine if their health information will be released, under what circumstances (e.g., any time or emergencies only), and by whom (e.g., health care providers, HIEs) [11].

Yet general consumer studies have shown concern regarding the ability to effectively maintain the privacy of one's personal information. The majority of those surveyed, in 2010, reported that patients do not want insurance companies to share or sell their information without explicit consent. Instead, consumers want the power to decide who can see their information and are interested in tools that would assist them in better managing how they consent [16].

Thus, a focused understanding of consent and information-sharing perceptions and behaviors is needed to assist in the development of algorithms and information services that can better support consumers in the effective brokering of their health data.

## 2.4 Impact on Digital Health Equity

Health equity aims to provide everyone an equal chance to attain the highest possible level of personal health and well-being. Medically vulnerable populations often face systemic barriers, such as limited access to quality healthcare and a lack of tailored healthcare resources [17]. This is equally true in terms of digital health tools, including PHIS [18]. For underserved and elderly populations, the issue of privacy (and trust) is crucial to PHIS utilization and requires significant attention due to a potential lack of understanding of the degree to which their health data can be

plundered, analyzed, and brokered without equal compensation. PHIS has the potential to become a powerful advocacy tool in these circumstances if developed with the needs of vulnerable populations in mind. When patients have a comprehensive record of their health history, they can more easily transition between care providers, reducing the risk of oversights or misdiagnoses. This empowerment enables individuals to make more informed decisions and engage in meaningful discussions about their healthcare.

Encouraging patients to participate more actively in their care plans can greatly improve health equity, enabling individuals to take control of their health management and address disparities in health outcomes. Engaged patients are more likely to follow treatment plans, attend follow-up appointments, and use preventive services, leading to better health outcomes and decreased healthcare costs. Financial incentives, such as reduced copayments or rewards for meeting health goals, can motivate patients, particularly those from underserved communities, to participate more fully in their care. This approach can bridge gaps in access to care and ensure that all patients, regardless of socioeconomic status, can optimize health outcomes. By incorporating patient feedback and tailoring care plans to meet the needs of diverse populations, healthcare providers can create more inclusive and effective care strategies, promoting greater health equity [19]. In this manner, PHIS are not just tools for managing personal health data but also catalysts for systemic change. By aligning personal health data with incentive and valuation models, we can catalyze a virtuous cycle. They empower individuals, especially the underserved, while the aggregated data informs systemic improvements in care delivery, public health policies, and financial models – ultimately enhancing health equity.

Early PHIS research findings related to the medically underserved identified important needs of patients and consumers in trusting that their personal health information was governed by laws that ensure that privacy and security protections would be inherent to its use. To be successful, these factors had to be addressed across personal, technical, organizational, and policy-related domains of healthcare [20]. In terms of personal health data-sharing, this is especially important due to the potentially wide degree of sharing required for patients working through multiple health systems and social service providers that may require greater latitudes of consent.

## 2.5 Impact on PHIS Adoption Requirements

Fintech and related blockchain technologies have the potential to transform the sharing, brokerage, and monetization of personal health data through incentivized participation. Studies have identified potential benefits (and challenges in the use of blockchain technologies in healthcare [21, 22, 23]. The opportunities for leveraging the blockchain within PHIS include its ability to assign unique transaction validations that link any individual piece of data

(e.g., clinical data or consent data) to an individual, which can support both the provenance and providence of the data. When implemented correctly, blockchain's secure and transparent framework can establish trust among patients, healthcare providers, and third parties by ensuring data integrity and privacy.

Blockchain supported smart contracts are self-executing agreements with the terms directly embedded in the code. By utilizing smart contracts within PHIS, patients could securely share their health data with researchers, pharmaceutical companies, and insurers in exchange for financial incentives or other rewards. These contracts could automatically enforce terms and conditions, ensuring that patients are compensated fairly [24]. Smart contracts can also reduce costs and improve the efficiency of healthcare delivery by eliminating the need for intermediaries. For example, blockchain-based platforms could use smart contracts to manage patient consent and ensure that data sharing is conducted ethically and transparently [25]. Increasing patient's trust in PHIS and providing fair remuneration for when their data is shared outside of health services received could assist in increasing patient activation and adoption.

## 3. Research Methodology

This study utilizes a non-experimental, cross-sectional design targeting U.S. adults across a wide range of demographic backgrounds, including age, income, ethnicity, and education. Participants were recruited through a web-based survey, which assumes that participants have a basic level of web experience and use of related technologies and, thus, would be familiar with e-consenting practices. The survey consisted of 22 questions, and all survey instruments were reviewed and approved by a sanctioned Institutional Review Board. Consequently, all survey respondents were given informed consent, and all data was anonymized. Survey instruments were aimed at measuring personal privacy and data-sharing experience questions that explored domains related to:

1. Data-sharing Habits
2. Privacy Policies and Consent Models
3. Personal Health Information Sharing
4. Incentives for Sharing

To assess the reliability or internal consistency of the survey questions, we employed the Cronbach's alpha statistical measure. We confirm that Cronbach's alpha for the items was greater than 0.70.

## 4. Results

Survey results gathered over one week resulted in 336 usable responses. Results span a range of online sharing topics, beginning first with an individual's inclination to

share specific types of personal data (e.g. social, financial, consumer, and health data). The study then shifts focus to comprehension and trust in data-sharing privacy policies. Explored next are these concepts within the domain of health information to understand what types of health data individuals currently share, with whom they share it, and the mechanisms by which these individuals share such information. The study concludes with an examination of incentives, if any, that may motivate individuals to share their health data.

### 4.1 Population

Detailed in Figure 1, survey results capture a diverse range of ages and represent a good subset of the U.S. population across multiple age ranges. Of those surveyed, 33% of respondents were over the age of 55, 46% were aged 35 to 54, and 21% were aged 18 to 34.

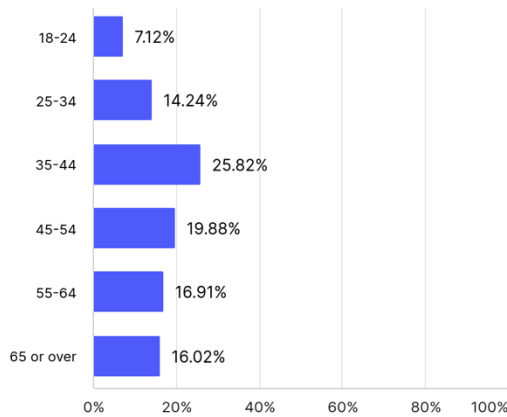


Figure 1. Demographics: Age (n=336)

Income distributions were also diverse. Detailed in Figure 2, 63% earn under 50k, 12% earning between 50k and 75k, and 25% earn 75k or more.

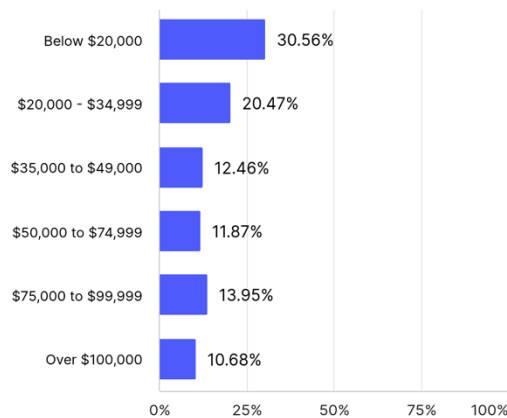


Figure 2. Demographics: Income (n=336)

Detailed in Figure 3, survey responses also tracked the highest level of education of participants. Results found that 59% of respondents identified high school as their highest level of education, while 31% reported college as their highest level of education. Only 7% reported having earned an advanced degree.

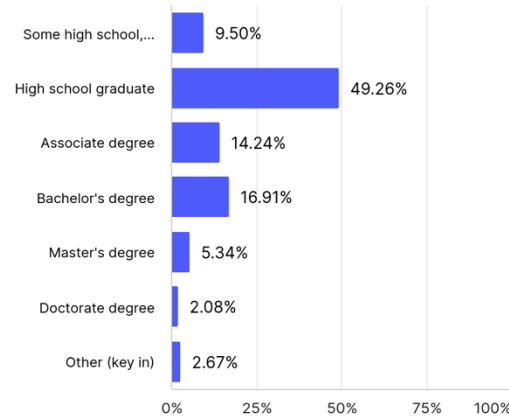


Figure 3. Demographics: Education (n=336)

### 4.2 Privacy Policies

Our next set of survey questions focused on privacy policies and how well users understand and trust data-sharing and privacy policies. Detailed in Figure 4, results show that most individuals understood privacy policies (37%) or at least got the general idea (45%). At the same time, a smaller percentage of respondents indicated that they did not understand them (10%). A smaller percentage of respondents stated that they do not read them at all (8%).

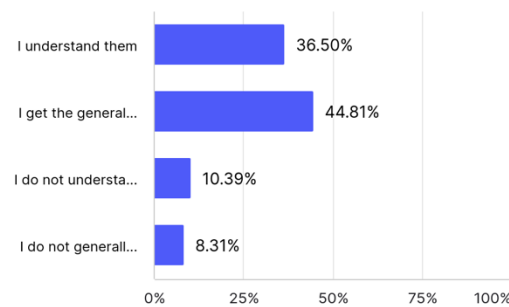
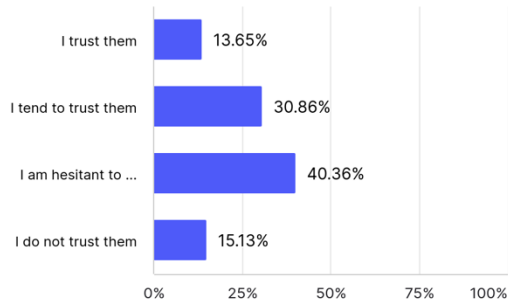


Figure 4. Data-sharing Policy: Comprehension

Survey responses tracked trust in data-sharing policies. Detailed in Figure 5, as it relates to trust in online data-sharing and privacy policies, most respondents were either hesitant to trust them (40%) or found them untrustworthy (15%). A smaller percentage of participants trusted them

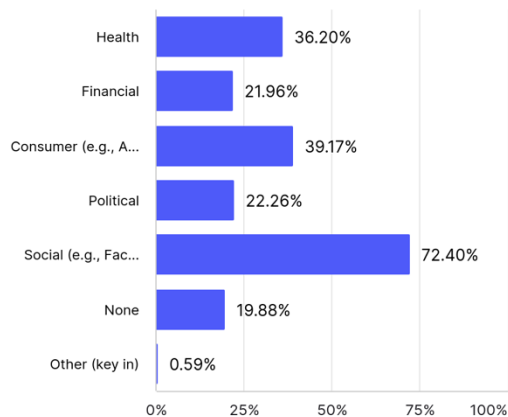
completely (14%), with some respondents only tending to trust them (31%).



**Figure 5. Data-sharing Policy: Trust**

### 4.3 Data-Sharing Trends (General)

Our next set of survey questions looked at overall online data-sharing trends as they relate to broad categories of data, including social, health, financial, consumer, and political data. Detailed in Figure 6, results found that a majority of respondents indicated having shared social data online (72%), while consumer data and health data rounded out the Top 3 categories at 39% and 36%, respectively.



**Figure 6. Data-sharing by Data Type**

A second question asked respondents what types of data they had concerns about sharing. Detailed in Table 1, survey responses indicated that financial data and health data were categories that respondents were very concerned about (67% and 45%, respectively). In comparison, political and social data were categories of least concern (40% and 23%, respectively).

**Table 1. Data-sharing Concerns by Data Type**

	Very concerned	Slightly concerned	Not at all concerned
Social (e.g., Facebook)	108 32.0%	150 44.5%	79 23.4%
Health	151 44.8%	125 37.1%	61 18.1%
Financial	224 66.5%	77 22.9%	36 10.7%
Consumer	98 29.1%	173 51.3%	66 19.6%
Political	94 27.9%	110 32.6%	133 39.5%

Analyzing the data based on participants' income levels, chi-square tests revealed three significant associations and one marginal association. First, there was a significant association between income levels and the likelihood of sharing health information online ( $X^2(5,336)=10.85, p=0.05$ ). Secondly, a significant association was found between income levels and the unwillingness to share health information with healthcare workers ( $X^2(5,336)=12.57, p=0.03$ ). Finally, income levels were significantly associated with the sharing of financial information ( $X^2(5,336)=11.98, p=0.04$ ). Additionally, a marginally significant association was observed between income levels and the sharing of consumer information online ( $X^2(5,336)=10.73, p=0.06$ ). These results suggest that income level significantly influences participants' willingness to share various types of information.

Significant associations were observed in several areas when the data was analyzed based on participants' age groups. There was a significant relationship between age and the unwillingness to share health information with healthcare workers ( $X^2(5,336)=11.78, p=0.04$ ), as well as between age and participants' understanding of online data-sharing policies ( $X^2(5,336)=11.02, p=0.05$ ). In terms of incentives for data sharing, significant associations were found between age and monetary incentives ( $X^2(5,336)=18.48, p=0.002$ ), better health outcomes ( $X^2(5,336)=10.86, p=0.05$ ), and the contribution to science ( $X^2(5,336)=14.37, p=0.01$ ). These findings indicate that age plays a potential role in shaping participants' attitudes toward data sharing and their responses to various incentives.

### 4.4 Data Security Concerns

A separate question asked respondents how well they trust the security of different types of data online. Detailed in Table 2, survey responses highlight financial and health data as categories where respondents felt data was most

secure (67% and 45%, respectively), while political and social data were categories that would be less secure (40% and 23%, respectively).

**Table 2. Data Security Concerns by Data Type**

	Very secure	Somewhat secure	Not secure
Social	44 13.1%	176 52.2%	117 34.7%
Health	98 29.1%	177 52.5%	62 18.4%
Financial	90 26.7%	152 45.1%	95 28.2%
Consumer	55 16.3%	196 58.2%	86 25.5%
Political	47 14.0%	180 53.4%	110 32.6%

**4.5 Data-sharing Trends (Health)**

A primary objective of this research was to offer a clearer picture of perceptions of data-sharing trends related to healthcare. Our first set of questions across this construct asked what general categories of health data participants would be most willing to share. Detailed in Table 3, respondents were most willing to share fitness data (56%) and lifestyle data (50%). Participants were more hesitant to share clinical (43%) and mental health data (40%).

**Table 3. Willingness to Share Health Data Types**

	Very willing	Hesitant but willing	Not willing
Clinical	144 42.7%	146 43.3%	47 14.0%
Mental health	143 42.4%	135 40.1%	59 17.5%
Fitness	189 56.1%	113 33.5%	35 10.4%
Lifestyle (e.g., smoking/alcohol/drug use)	168 49.9%	125 37.1%	44 13.1%

The next set of questions focused specifically on health information-sharing practices, specifically health-related data captured in health document exchange standards (e.g., Allergies, Conditions, Medications, Procedures, Labs, Encounters, and Immunizations). Detailed in Table 4, respondents were generally willing to share many forms of health-related information. Respondents indicated that they

were very willing to share allergy-related (62%) and immunization-related data (53%), while they were not as willing to share encounters (24%) and mental health (21%) data.

**Table 4. Willingness to Share (Clinical Document Architecture)**

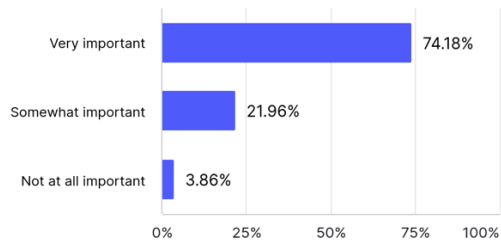
	Very willing	Hesitant but willing	Not willing
Medications	153 45.4%	128 38.0%	56 16.6%
Allergies	211 62.6%	97 28.8%	29 8.6%
Conditions	139 41.3%	149 44.2%	49 14.5%
Procedures	151 44.8%	136 40.4%	50 14.8%
Encounters	110 32.6%	145 43.0%	82 24.3%
Tests/Labs	136 40.4%	133 39.5%	68 20.2%
Immunizations	180 53.4%	105 31.2%	52 15.4%
Mental Health	129 38.3%	135 40.1%	73 21.7%

Participants were also asked who they would be most willing to share their health data with. Detailed in Table 5, the majority of respondents were most willing to share health data with healthcare professionals (58%) and family (57%). Respondents were hesitant but willing to share with research organizations (56%), legal aids (46%), and social workers (46%). Respondents indicated that they would be least likely to share health information with clergy.

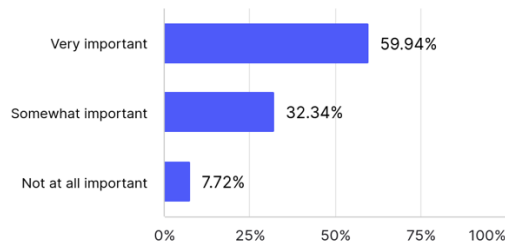
**Table 5. Willingness to Share Health Data With**

	Very willing	Hesitant but willing	Not willing
Healthcare Workers	195 57.9%	110 32.6%	32 9.5%
Research Organizations	81 24.0%	189 56.1%	67 19.9%
Family	193 57.3%	108 32.0%	36 10.7%
Clergy	80 23.7%	148 43.9%	109 32.3%
Legal Aids	106 31.4%	155 46.0%	76 22.6%
Social Workers	102 30.3%	156 46.3%	79 23.4%

Survey questions also asked respondents on the importance of knowing who information was shared with and if the ability to see a data-sharing history was important. Detailed in Figure 7, 74% of respondents stated that it was important to know who information was shared with, and 22% of respondents indicated that it was somewhat important. Detailed in Figure 8, 60% of respondents indicated that it was very important to see a history of shared data, while 32% stated it was somewhat important.



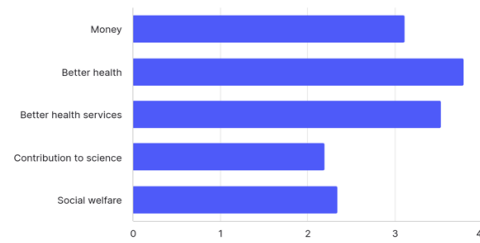
**Figure 7. Importance Of Knowing Who Information Is Shared With**



**Figure 8. Importance of Sharing History**

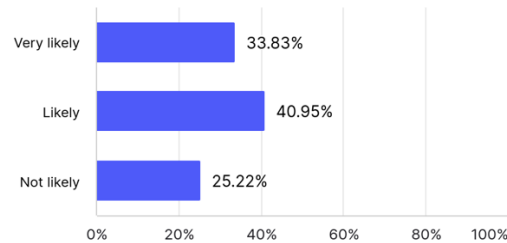
#### 4.6 Incentives for Data Sharing

Our final group of survey items focuses on incentives and how willing individuals are to share personal health information if given an appropriate incentive to do so. Incentives included money, better health, better health services, contribution to science, and social welfare. Detailed in Figure 9 are the respondent’s preferred incentives, ranked from most preferred (1) to least preferred (5). Individuals’ Top 3 preferred incentives were 1) overall better health, 2) better personalized health services, and 3) money.

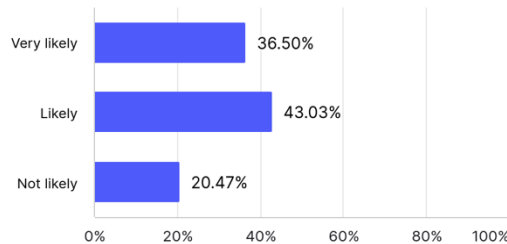


**Figure 9. Incentives Preferences**

Survey questions also asked how incentives could motivate individuals to share more. Detailed in Figure 10, most respondents stated they were very likely (34%) or likely (41%) to share data based on their preferred incentive method. Detailed in Figure 11, respondents were more likely to share as the incentives were increased, with 37% very likely to share and 43% likely to share.



**Figure 10. Incentives as Motivation**



**Figure 11. Increased Incentives Impact on Motivation**

## 5. Discussion

This research acknowledges that data-sharing, specifically health-related data-sharing, can be a double-edged sword. While there are inherent risks associated with providing consent to share, tangible benefits can be achieved in doing so. Effective data-sharing can lead to improved care continuity and enhanced communication among healthcare providers, which are crucial for patient outcomes. Care continuity ensures that patients receive consistent and coherent treatment over time and distance, reducing the likelihood of medical errors and improving overall health

management. Enhanced communication among healthcare providers facilitates better coordination, timely interventions, and a more comprehensive understanding of a patient's medical history, all of which contribute to higher-quality care. In this research, we explore perceptions of data-sharing trends, data-sharing policies, and incentive models for data-sharing.

## 5.1 Privacy Policies and Consent Models

It has been over two decades since the term Web 2.0 was coined, and today's Internet is largely supported by user-generated data. Consequently, today's most popular systems, such as YouTube and TikTok, require their users to agree to their ToS. An initial objective of this research focused on users' general awareness of ToS agreements, EULAs, etc., as well as the data-sharing models and privacy policies they adopt. What we discovered was surprising. Overall, 80% of respondents surveyed indicated that they understand these policies and get the general idea. However, over 55% responded that they were hesitant to trust these policies or do not trust them at all. This is largely concerning for two reasons. First, it means users are agreeing to an organization's ToS simply as a condition to use a system. Second, it imparts a sense of resignation on the user's part in that they lack control over the data they are generating. Within the healthcare industry and other highly sensitive and personal information spaces, this lack of trust can have adverse effects, which we will address in Section 5.2.

Our results reinforce the current gap that exists in the absence of guidance, models, and/or schemas, which will allow developers to easily implement PGHD consent models that can help users navigate consent within the consumer space. Such models need to help users navigate consent across data-sharing domains related to the data type and domain of health data, the entity, medium, media, frequency, time, situation, and market. This space requires a different type of consent navigation than the provider space and will be crucial not only as it relates to the privacy preferences of the individual but also in terms of the opportunity for PGHD to contribute to the health of the individual.

Within the HIT space, models and frameworks are needed to help navigate the complexities of patient-generated consent requirements and the nuances described by each chain within the data-sharing transaction. Care providers, HIT vendors, and policymakers need models and frameworks that allow for a more standardized approach to adopting, managing, and enforcing personal consent policies. Informed by current consent models of consumer information service standards, social-network standards (Facebook, Amazon, etc.), and a survey of frequently vulnerable populations, including the elderly and underserved, this study provides findings that help to inform consumer and patient advocacy organizations, policymakers

and vendors as to the perceptions and practices of consumers of personal health information.

It is important to examine how individuals treat information-sharing policies to ensure users understand what it means to 'share' information and what it means in the age of big data and generative AI, particularly when it comes to more sensitive information, such as the case with personal and mental health.

## 5.2 Data-sharing

The results of this research identified that social data was the most shared type of data online. This should come as no surprise considering the widespread migration away from one-to-one communication platforms such as email to those platforms that provide enhanced sharing capabilities, such as Facebook, YouTube, and Instagram. However, due to their sheer popularity and immense footprints, as well as their focus on advertising revenue, these platforms face tremendous scrutiny for how they view and handle the personal information of their online subscribers.

Regarding health-specific data, only 36% of respondents indicated sharing such data. Yet, the trajectory for PGHD is growing as PHIS systems are more widely accepted, as are IoT health monitoring devices and fitness apps. For lessons learned, PHIS platforms should keep a close eye on how the public perceives data-sharing across widely used social networking platforms. As identified in this research, users are more hesitant to share personally sensitive information compared to social data. Across our population, respondents cited concern over the safety of PHIS, with 82% very concerned or slightly concerned with sharing such data. Yet respondents identified that they are very willing (58%), or hesitant but willing (33%) to share data with covered entities such as healthcare professionals.

Based on post-hoc contingency table analyses, participants in the 18-24 and 25-34 groups were less likely to share health information online when compared to the other age groups. Moreover, participants in the 65 or over group were more likely to accept monetary incentives to share their personal health information when compared to the other age group. Finally, the least likely group to accept monetary incentives was the 18-24 age group.

Although this study does not explore mitigating factors for these apprehensions, we can surmise that levels of trust, privacy, and security were all factors as identified in prior research [26, 27, 28]. This highlights the need for broader frameworks and models to effectively integrate PGHD as a valuable resource for clinical decision-making. When PGHD is timely and accurately integrated, it can facilitate quicker interventions, improve patient outcomes, and enable personalized care plans. For instance, in scenarios such as remote management of pharmaceuticals and monitoring



medication adherence, integrated data can significantly improve clinical decision-making [29].

Regardless of the motivating factors for health information sharing, PHIS vendors and providers would benefit significantly in building systems that help manage consent preferences. An individual's feelings of control over their personal health information can be an integral component in that individual's overall health behavior. To be effective, PHIS must earn the trust of an individual, whereby the information shared by its users is used to facilitate that individual's healthy outcomes. Within this research, it was identified that while face-to-face communication was the most preferred method for sharing information, Internet technologies were the second most preferred method, indicating the potential for increased adoption within underserved populations. Adoption will likely be tempered, however, by factors such as trust. Survey results found that while most participants read and felt as though they understood data-sharing and privacy policies, there was a lack of trust in what was being stated within these policies. This research has important implications for practitioners looking to implement PHIS within underserved populations and provides a baseline for building greater knowledge of information sharing and e-consent behaviors.

### 5.3 Incentives

Recent research has reinforced the importance of higher levels of trust while mitigating risk as important factors in a shared model of healthcare, where healthcare organizations and individuals are partners [30]. What we found in this research was that while respondents were less inclined to share health-related data, respondents identified improved health outcomes as the primary reason to share personal health information. This trend is a positive step towards wider PHIS adoption. It highlights potential motivation to increasingly use personal health data in efforts to attain personal health goals and see benefits in engaging others with their data. With that said, not all individuals cited health outcomes as their primary motivator, and many participants indicated that financial incentives could play an essential role in sharing personal health data.

### 5.4 PHIS Adoption and Diffusion

As identified in survey findings, participants had differing sensitivities in relation to sharing both the types of health data (i.e., health, mental, fitness) and clinical data types (i.e., allergies, encounters, medications). To date, HIE generally shares clinical summaries wholesale outside of some exclusions, such as information related to substance use as dictated in Title 42 CFR Part 2 [31]. To effectively manage and interpret information-sharing consent within personal health information systems, especially as consent varies over time, more advanced methods for tracking and

segmenting consent will be necessary. As discussed in section 2.5 of the background, improved PHIS design could help further support data-sharing within the domain of PGHD. This might include the ability of blockchain technologies to more sustainably record and provide a history of healthcare transactions, which would offer advantages in reducing the fraudulent use of PGHD, as well as providing the opportunity to record patient-federated sharing transactions and incentivize adoption and greater diffusion across patient and consumer populations.

## 6. Conclusion

As individuals take greater control of their personal health information and begin utilizing online systems to help manage this information, it becomes imperative to continue to examine how individuals share information online and their perceptions of online sharing policies. This is particularly important for individuals who are hesitant to share personal health data, even when it is in their best interests to do so. In this research, we explored data-sharing behaviors and perceptions across a representative sample of U.S. adults. Findings identified an overall sense of apprehension towards online data-sharing and privacy policies, and yet a willingness to share personal information, including health data, when proper health incentives exist. More so, we argue that any responsible PHIS, one that truly promotes healthy behaviors, will ensure reasonable protection from uninitiated or unknowing oversharing of personal health data and will encourage and empower individuals to share the correct information at the right time.

## 7. References

- [1] Angst, CM, and Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, 33(2), pp. 339–370.
- [2] McClain, C., Faverio, M., Anderson, M., and Park, E. (2023). How Americans View Data Privacy The role of technology companies, AI and regulation – plus personal experiences with data breaches, passwords, cybersecurity and privacy policies, *Pew Research Center*.
- [3] Auxier, B. Rainie, L., Anderson, M., Perrin, A., Kumar, M., and Turner, E. (2019). Americans And Privacy: Concerned, Confused and Feeling Lack Of Control Over Their Personal Information, *Pew Research Center*.
- [4] Hulsén, T. (2020). Sharing Is Caring—Data Sharing Initiatives in Healthcare, *International Journal of Environmental Research and Public Health*, 17(9).
- [5] Hudson KL and Collins FS (2017). The 21st Century Cures Act — A view from the NIH. *The New England Journal of Medicine*. 2017, 376(2), pp. 111-113.

- [6] Marquard, JL, Garber, L., Saver B., Amster, B., Kelleher, M., and Preusse, P. (2013). Overcoming challenges integrating patient-generated data into the clinical EHR: Lessons from the CONTrolling Disease Using Inexpensive IT - Hypertension in Diabetes (CONDUIT-HID) Project, *International Journal of Medical Informatics*, 82(10), pp. 903-910.
- [7] Braunstein ML (2018). Healthcare in the age of interoperability: the promise of fast healthcare interoperability resources, *IEEE Pulse*, 9(6), pp. 24–27.
- [8] Eliyan, AF, Marwat, SNK, Qadir, J., and Al-Fuqaha, A. (2024). Informed Consent in IoT Environments: Challenges and a Futuristic Incentives-Based Model, *IEEE Internet of Things Magazine*, 7(1), pp. 112-119.
- [9] Kennedy, E. and Kassebaum, N. (1996). Health Insurance Portability and Accountability Act, Public Law 104-191. U. S. Congress.
- [10] Office of the National Coordinator (2015). 2015 Edition Final Rule: Data Segmentation for Privacy (DS4P), U.S. Department of Health and Human Services, Washington, DC: U.S. Government Printing Office. Retrieved online on August 21, 2024, from [https://www.healthit.gov/sites/default/files/2015editionehrcertificationcriteria4p\\_10615.pdf](https://www.healthit.gov/sites/default/files/2015editionehrcertificationcriteria4p_10615.pdf).
- [11] Office of the National Coordinator (2024). Meaningful Consent Overview, U.S. Department of Health and Human Services, Washington, DC: U.S. Government Printing Office. Retrieved online on August 21, 2024 from <https://www.healthit.gov/topic/meaningful-consent-overview>.
- [12] Theodos K. and Sittig S. (2020). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply, *Perspectives in Health Information Management*. 18(11).
- [13] Office of the National Coordinator for Health Information Technology (2016). Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA, U.S. Department of Health and Human Services, Washington, DC: U.S. Government Printing Office. Retrieved online on August 21, 2024, from [https://www.healthit.gov/sites/default/files/non-covered\\_entities\\_report\\_june\\_17\\_2016.pdf](https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf).
- [14] Backonja U., Kim K. and Casper GR (2012). Observations of daily living: Putting the “Personal” in personal health records, *Proceedings of the 11th International Congress on Nursing Informatics*, 2012(6).
- [15] Przybylski, M. (2010). Health locus of control theory in diabetes: a worthwhile approach in managing diabetic foot ulcers?, *Journal of Wound Care*, 19(6), pp. 228-233.
- [16] Zogby International. (2010). Patient Privacy Poll. Retrieved online on August 21, 2024, from <https://patientprivacyrights.org/wp-content/uploads/2010/11/Zogby-Result-Illustrations.pdf>.
- [17] Lyles CR, Nguyen OK, Khoong EC, Aguilera A., and Sarkar U. (2023). Multilevel Determinants of Digital Health Equity: A Literature Synthesis to Advance the Field. *Annual Review of Public Health*, 44, pp. 383-405.
- [18] Shaw J. and Glover W. (2024). The Political Economy of Digital Health Equity: Structural Analysis, *Journal of Medical Internet Research*, 26.
- [19] Simon M., Baur C., Guastello S., Ramiah K., Tuft J., Wisdom K., Johnston-Fleece M., Cupito A., and Anise A. (2020). Patient and Family Engaged Care: An Essential Element of Health Equity. *NAM Perspectives*.
- [20] Botts, N., Horan, T., and Thoms, B. (2011). HealthATM: Personal health cyberinfrastructure for underserved populations, *American Journal of Preventive Medicine*, 40(5), pp. 115-112.
- [21] Chinnasamy P., Albakri A., Khan M., Raja AA, Kiran A., and Babu JC (2023). Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System, *Applied Sciences*. 13(6), 3970.
- [22] Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., and Oropallo, E. (2023), Blockchain’s coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem, *Technovation*, 120(C).
- [23] Saeed H., Malik H., Bashir U., Ahmad A., Riaz S., Ilyas M., Bukhari WA, and Khan MIA (2022). “Blockchain technology in healthcare: A systematic review,” *PLoS One*, 17(4).
- [24] Elvas LB, Serrão C, and Ferreira JC (2023). Sharing Health Information Using a Blockchain. *Healthcare (Basel)*, 11(2), p. 170.
- [25] Kim K., Kim SM, Park Y., Lee E., Jung S., Kang J., An D., Min K., Shim SR, Yu HW, and Han HW (2024). A Blockchain-based Healthcare Data Marketplace: Prototype and Demonstration, *JAMIA Open*, 7(2).
- [26] Carrión, S. Fernández-Alemán, JL, and Toval, A. (2012). Are personal health records safe? A review of free web-accessible personal health record privacy policies,” *Journal of Medical Internet Research*, 14(4).
- [27] Perera, G., Holbrook, A., Thabane, L., Foster, G., and Willison, DJ (2011). Views on health information sharing and privacy from primary care practices using electronic medical records, *International Journal of Medical Informatics*, 80(2), pp. 94–101.
- [28] Chin, E., Porter-Felt, A., Sekar, V., and Wagner, D. (2012). Measuring user confidence in smartphone security and privacy, *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*, ACM, New York, NY, USA, pp. 1-16.
- [29] Singh, N., Varshney, U., and Sarkar, S. (2022). Patient Generated Health Data: Framework for Decision Making, *Proceedings of the 55th Hawaii International Conference on System Sciences*, January 4-7, 2022.
- [30] Liu K. and Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services, *Computers in Human Behavior*, 127, 107026.
- [31] Campbell, ANC, McCarty, D., Rieckmann, T., McNeely, J., Rotrosen, J., Wu, LT, and Bart, G. (2019). Interpretation and integration of the federal substance use privacy protection rule in integrated health systems: A qualitative analysis, *Journal of Substance Abuse Treatment*, 97, pp. 41-46.