MILKEN INSTITUTE
FasterCures

Landscape of Trust:
Health Data Frameworks

HADLY CLARK AND JESSICA MARSHALL

About the Milken Institute

The Milken Institute is a nonprofit, nonpartisan think tank.

We catalyze practical, scalable solutions to global challenges by connecting human, financial, and educational resources to those who need them. We leverage the expertise and insight gained through research and the convening of top experts, innovators, and influencers from different backgrounds and competing viewpoints to construct programs and policy initiatives. Our goal is to help people build meaningful lives in which they can experience health and well-being, pursue effective education and gainful employment, and access the resources required to create ever-expanding opportunities for themselves and their broader communities.

About FasterCures

FasterCures, a center of the Milken Institute, is working to build a system that is effective, efficient, and driven by a clear vision: patient needs above all else. We believe that transformative and life-saving science should be fully realized and deliver better treatments to the people who need them.

Introduction

The rapid advancement of the health technology landscape relies heavily on patient data. Patient data from medical records and digital health apps can be leveraged to build new tools that can help diagnose disease, remotely monitor and track patients, and make groundbreaking discoveries that lead to new treatments and cures. Data-reliant entities, such as technology companies, have the most advanced capabilities to aggregate and analyze these data. But, because their activities fall outside of the traditional authority that governs health data privacy, their participation carries substantial implications for how patient data are collected and used.

The Pew Research Center, which publishes an annual survey to measure social trust, defines trust as a "belief in the honesty, integrity, and reliability of others—a 'faith in people.'"[1] The 2022 annual Edelman Trust Barometer found that distrust is the default for the majority of people. Fifty-nine percent of respondents indicate they tend to distrust until they see evidence that something is trustworthy versus a tendency to trust until they see evidence that something is untrustworthy.[2] According to a poll of 2,200 adults across the country, fewer than three in five Americans trust the US health-care system. Further, trust in the scientific community has eroded since this tracking began in November 2020.[3]

These survey results tell us that trust is elusive and must be earned. Controversies around the use of health data persist and undermine efforts to restore and build trust. Many data-reliant organizations have been rebuked for their handling of patient data and have had to walk back controversial partnerships. This January, the suicide hotline nonprofit, Crisis Text Line, came under fire for its data-sharing relationship with a for-profit company, Loris.ai, for ethics and privacy concerns.[4] Users of the service were concerned the data shared were not truly anonymized.[5]

Health data are currently protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[6] HIPAA ensures patient control of health data that are captured in electronic health records or among a patient, provider, or health system. Data protected under HIPAA cannot be used for purposes without the patient's explicit consent. However, HIPAA does not cover health data that patients enter or share with mobile apps, websites, or online tools outside of the realm of the patient-provider relationship. This gap in federal policy has led to a proliferation of exploitive data practices without explicit patient consent or knowledge.

Moving Toward a Trusted System

To move toward a system that patients trust, we must paint a clear picture of the desired system. In late 2020, FasterCures brought together experts who work with patient data in various settings to outline key elements of a trusted system. Part of the work was to envision the aspects needed to establish trust. Experts identified three foundational components of trust. For this report, we focus on one of the elements: the need to create strong and clear protections for patient data. The other two elements—ensuring that patients reap benefits from contributing their data and creating safe platforms and spaces for peer groups—are also crucial and will be addressed in our ongoing work.

The proliferation of online tools and mobile applications that rely on health data outside of the traditional patient-provider relationship has highlighted the need to consider how health data outside the provider realm are protected. Protections for patients under HIPAA do not apply to data captured in health-focused mobile phone applications, websites, or digital tools that are not used within a health system, by a provider, or as part of a clinical study.

Demonstrating thoughtful and intentional work to address the many and multifaceted risks of sharing health data is an integral part of building trust with the patient community. Data-reliant entities that collect and use health data should carefully determine what data may be obtained pursuant to informed consent agreements and establish processes to ensure that these agreements comply with appropriate regulations and function correctly. Structural data protections should support these efforts; if HIPAA does not fully protect the data used, then other guardrails should be established to build confidence that such data will not be misused.

Health Data Trust Frameworks

Numerous trust frameworks have emerged that seek to provide standards or guidelines on the collection and use of health data. These frameworks have been developed for different actors in the system, including physicians, health information exchanges, and app developers. Because the frameworks are intended for different audiences, we recognize the challenges to comparability. In this exercise, we sought not to compare these frameworks to each other but rather to identify standards that can be more widely adopted by others and to suggest future areas into which frameworks can expand. Through our research, we identified eight frameworks that cover health data. The list is not exhaustive because we limited our review to publicly available frameworks that cover the consumer-directed exchange of health data or data that are requested under an individual's right under HIPAA to invoke access to their health records or information drafted within the past 10 years.

Framework Landscape

FRAMEWORK	FRAMEWORK DEVELOPER	DESCRIPTION
Carequality Trust Framework	*Healtheway*	The framework is designed to establish trust among health information exchanges participating as Carequality Implementers and promote the electronic exchange of health information through the standardized requirements.[7]
Consumer Privacy Framework for Health Data	*Center for Democracy & Technology/ eHealth Initiative & Foundation*	The framework has a proposed self-regulatory structure for non-HIPAA health-care-related data focused on accountability. It is designed to hold participating entities to a set of standards separately developed through a multistakeholder process.[8]
Guiding Principles for the Privacy of Personal Health Data	*Consumer Technology Association*	The principles serve as a set of baseline recommendations to develop and implement personal health technologies, products, and services to mitigate risks that consumers may perceive concerning their health data.[9]
Trust Framework & Code of Conduct	*The CARIN Alliance*	The Code of Conduct is meant to provide patients with an understanding of how their health data are being used by all patient-facing applications, regardless of whether HIPAA covers them.[10]
The Trusted Exchange Framework	*Office of the National Coordinator for Health IT*	The framework describes a common set of principles that facilitate trust between health information networks. These principles serve as "rules of the road" for nationwide electronic health information exchange.[11]
Trust Framework for Health Information Exchange	*National Health Information Exchange Governance Forum*	The framework is for governing entities and their participants to share trust attributes to support exchange with a group of unaffiliated entities.[12]
mHealth App Guidelines	*Xcertia*	The guidelines were developed with a shared purpose to provide a level of assurance to clinicians and consumers alike. The mobile health apps that comply with the guidelines are vetted to deliver value to the user.[13]
Privacy Principles	*American Medical Association*	The principles are meant to apply to entities other than those already considered covered entities under HIPAA. The principles provide individuals with rights and protections from discrimination and shift the responsibility for privacy from individuals to data holders, unless it is a HIPAA-covered entity.[14]

Source: Milken Institute (2022)

Discussion

Protection of health data is fundamental to a well-functioning biomedical ecosystem. As such, many of the standards in the frameworks we reviewed relate to the essential elements of *privacy*—what rights patients have to control their data— and *security*—how health data are protected.

Each framework guides privacy policies that are based on best practices, made publicly available, and are easy to read. Additional similarities across the frameworks include the following:

- Limiting the collection of data to only what patients expressly permit was included in six of the frameworks included in our review. This means that data-reliant entities cannot collect any data without first getting permission from patients.
- Inclusion of versions of the "right to be forgotten" were in five of the frameworks we reviewed. The "right to be forgotten" allows patients who no longer wish to have their data used or collected by the application removed.

Areas to Strengthen

Although these frameworks speak to some of the more fundamental aspects of health data protections, such as privacy and security, we identified three areas that could be strengthened or expanded by the framework developers. These areas seek to provide clarity to patients on what data are collected, how they are used, and who they are shared with, as well as to prevent discriminatory use of health data.

Provide clear and transparent data policies:

- Clear and transparent data policies where patients are informed of what data are collected or shared with third parties, in addition to knowing what data are collected passively, collected on a one-time basis, or collected persistently, were included in three frameworks.

Studies have shown that patients and application users are often not aware that data are being collected passively or sold to third parties—including advertisers. For example, according to a recent study published in the *Journal of the American Medical Association*, smartphone applications infrequently communicate to patients the terms in which their health data are used or disclosed, and 81 percent of the apps reviewed in the study transmitted data for advertising and marketing purposes or analytics to third parties.[15]

The frameworks included in this report rely heavily on federal and state privacy policies to inform their standards. However, we know based on our research that patients want their health data to be safe, but importantly, they want to understand how their data are protected. Although all the frameworks included in our landscape had strong privacy protections, the information is often buried in "terms of use" clauses, written in legalese difficult for average Americans to understand. These protections also did not ensure the transparent communication of how or by whom their health data would be used—including collection, use, and aggregation.

Patients should be aware of what data are being collected and how their data are being used at all times. This information should be not only clearly communicated but also easy to find online, within the native application or per the individual's request.

Some of the frameworks we reviewed address this issue and offer standards to help provide guidance on this. For example, the framework co-developed by the Center for Democracy and Technology (CDT), which champions individual rights and privacy, and the eHealth Initiative (eHI), an independent nonprofit that specializes in health information technology, instructs data-reliant entities to provide patients with "free, clear, and easy" ways in which they can request a list of all organizations or third parties that have received, licensed, or even purchased their consumer health information.[16] Frequently, health data use extends beyond the original application or platform that patients initially engage with. The CARIN Alliance Framework and Code of Conduct expand on the guidance in CDT's framework to include the right for patients to change their preferences of whom receives their health data.[17]

Although several of the frameworks included in our review do have principles that promote transparency, there was a lack of explicit guidance on how to implement "transparent data sharing" policies that patients could accurately understand and quickly find. Patients should be able to quickly and easily locate data-sharing practices in the application, website, or tool. The policies should be written in plain, non-legal language at a level that most Americans can understand. When the guidance is updated, patients should be informed through their preferred method of communication previously agreed to. At any time, patients should be able to reference these practices and contact a member of the organization for further clarification.

Notification of breach of security:

- ***Notifying patients of a data breach was included in half of the frameworks.***

In addition to transparent data sharing policies, patients should be quickly informed if their data are used, viewed, or acquired by an unauthorized party. If security is breached, the entities should promptly notify all of their patients so they are aware of the breach and what personal data were exposed. Patients should also be informed of what action, if any, should be taken on their part.

Half of the frameworks included in our review included breach notification guidance in accordance with existing state or federal laws such as those in the Consumer Technology Association's (CTA) Guiding Principles.[18] For data outside of the jurisdiction of HIPAA, such as data shared through mobile applications, wearables, and websites, the Federal Trade Commission (FTC) enforces the Health Breach Notification Rule requiring all entities to inform patients if their data have been disclosed or acquired without the patient's permission.[19] In some cases, the FTC stipulates that the media also be informed of the breach in addition to patients and the FTC.[20]

Patients should be informed in a timely fashion if their data are disclosed or acquired without their permission

The CARIN Alliance's framework specifies that in addition to the notification of patients of a breach, data-reliant entities should also "provide meaningful remedies to address breaches, privacy, or other violations incurred because of misuse of the patient's health information."[21] Similarly, the CTA's Guiding Principles provide preventive measures reminding patients of the shared responsibility to maintain the privacy of personal health data, including patients selecting strong passwords and not sharing passwords.[22]

Several of the frameworks also emphasized the importance of informing patients of a data breach in a timely manner. Xcertia's framework provides specific guidance that in the event of a data breach, patients must be notified no later than one month after the incident. Patients must also be informed of what type of data was breached and whether any third party or international organizations accessed the data.[23]

Even though the FTC's Health Breach Notification Rule was enacted over a decade ago, it has never been enforced. To provide additional clarification of the rule's scope and put entities on notice, the FTC released a Policy Statement in late 2021.[24]

Prevent discriminatory use:

- ***Half of the frameworks contained anti-discrimination protections.***

Another component of strong data protections is the prevention of harm caused by discrimination, stigmatization, or profiling of data shared by patients through digital tools and applications. To the extent possible, entities should mitigate any potential algorithmic bias by ensuring patients' health data will not be collected or used against them in any way. This is especially relevant to vulnerable or high-risk communities because certain widely used algorithms affecting millions of patients exhibit significant bias that can exacerbate existing health and social inequities.[25]

Framework developers can mitigate biased algorithmic development by including guidance that prevents the exploitation of one's health data. We see this in the inclusion of anti-discrimination protections in some of the frameworks included in our landscape. The American Medical Association's (AMA) anti-discrimination principles protect individual patients from "discrimination, stigmatization, discriminatory profiling, and exploitation occurring during collection and processing of data, and resulting from use and sharing of data, with particular attention paid to minoritized and marginalized (vulnerable) communities."[26]

Guidance should be included that prevents entities from using an individual's health data against them in any way, including but not limited to collection, disclosure, or use of an individual's health data to discriminate.

As stated in the CDT and eHI Foundation Consumer Privacy Framework for Health Data, these protections should also extend to an individual's "refusal to use or cessation of use of a particular platform, product, app, or digital health tool, that could lead to discrimination, stigmatization, harmful profiling, or exploitation."[27] These protections are designed to prevent entities from collecting, disclosing, or using patient or consumer health data to train or subject to any automated, algorithmic, or artificial intelligence (AI) application unless express consent from the patient or consumer is obtained. These protections stipulate that any automated processes or systems must also mitigate any potential algorithmic bias, requiring measures to prevent bias throughout the design process, encourage transparency, and include routine auditing.

Anti-discrimination protections should extend to developing, training, and using AI applications, as seen in the CDT and eHI Foundation framework. Individuals

should be made aware through appropriate and express informed consent practices. Just as the AMA included in its Privacy Principles, individuals should have the right to know whether their health data will be used to develop or even train machines or algorithms, and opportunities to participate in data collection for these purposes must be on an opt-in, not opt-out basis.[28]

Conclusion

Our landscape of trust frameworks in the health data space found that the current frameworks heavily rely upon the regulatory schema that provides protections against exploiting the vulnerabilities caused by security or privacy breaches. Getting these health data frameworks right alone will not build trust and confidence with patients. However, it is a step toward offering a view on how a company can begin that process. And the work needs to continue. Creating more robust frameworks is one step of many toward a trusted system.

Endnotes

1. *Americans and Social Trust: Who, Where and Why* (Pew Research Center, February 22, 2007), https://www.pewresearch.org/social-trends/2007/02/22/americans-and-social-trust-who-where-and-why/.
2. *2022 Edelman Trust Barometer* (Edelman, 2022), https://www.edelman.com/trust/2022-trust-barometer.
3. "Tracking Trust in US Institutions" *Morning Consult*, January 6, 2022, https://morningconsult.com/tracking-trust-in-institutions/.
4. Alexandra S. Levine, "Suicide Hotline Shares Data with For-Profit Spinoff, Raising Ethical Questions," *Politico*, January 28, 2022, https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617.
5. Charlotte Jee, "You're Very Easy to Track Down, Even When Your Data Has Been Anonymized," *Technology Review*, July 23, 2019, https://www.technologyreview.com/2019/07/23/134090/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized/.
6. "HIPAA Enforcement," US Department of Health & Human Services, accessed February 8, 2022, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.
7. *Carequality Trust Framework* (Healtheway, 2015), https://sequoiaproject.org/wp-content/uploads/2015/01/Carequality_Principles-of-Trust_Final_Carequality-template.pdf.
8. *Consumer Privacy Framework for Health Data* (Center for Democracy & Technology and eHealth Initiative & Foundation, February 2021), https://cdt.org/wp-content/uploads/2021/02/2021-02-09-CDT-and-eHI-Proposed-Consumer-Privacy-Framework-for-Health-Data-d-FINAL.pdf.
9. *Guiding Principles for the Privacy of Health Data* (Consumer Technology Association, 2021), https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf.

10. *Framework & Code of Conduct, Version 2.0* (CARIN Alliance, May 2020), https://www.carinalliance.com/wp-content/uploads/2020/07/2020_CARIN_Code_of_Conduct_May-2020.pdf.

11. "Trusted Exchange Framework and Common Agreement (TEFCA)," Office of the National Coordinator for Health Information Technology, accessed January 18, 2022, https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement-tefca.

12. *Trust Framework for Health Information Exchange* (National HIE Governance Forum, December 2013), https://www.c4tbh.org/wp-content/uploads/2020/04/ONC-trust-framework13-Trust-Framework-for-HIE.pdf.

13. *mHealth App Guidelines* (Xcertia, August 12, 2019), https://www.himss.org/sites/hde/files/media/file/2020/04/17/xcertia-guidelines-2019-final.pdf.

14. *AMA Privacy Principles* (American Medical Association, 2020), https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf.

15. K. Huckvale, J. Torous, and M. E. Larsen. "Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation." *JAMA Netw Open*. 2(4):e192542 (2019). https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782.

16. *Consumer Privacy Framework for Health Data* (Center for Democracy & Technology and eHealth Initiative & Foundation).

17. *Framework & Code of Conduct*, Version 2.0 (CARIN Alliance).

18. *Guiding Principles for the Privacy of Health Data* (Consumer Technology Association).

19. "Health Breach Notification Rule 16 CFR Part 318," Federal Trade Commission, accessed February 22, 2022, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule.

20. "FTC Warns Health Apps and Connected Device Companies to Comply with Health Data Breach Notification Rule," Federal Trade Commission, September 15, 2021, https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health.

21. *Framework & Code of Conduct*, Version 2.0 (CARIN Alliance).

22. *Guiding Principles for the Privacy of Health Data* (Consumer Technology Association).

23. *mHealth App Guidelines* (Xcertia).

24. *Statement of the Commission, on Breaches by Health Apps and Other Connected Devices* (Federal Trade Commission, September 15, 2021), https://www.ftc.gov/public-statements/2021/09/statement-commission-breaches-health-apps-other-connected-devices.

25. Z. Obermeyer et al., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* (October 25, 2019), https://pubmed.ncbi.nlm.nih.gov/31649194/.

26. *AMA Privacy Principles* (American Medical Association).

27. *Consumer Privacy Framework for Health Data* (Center for Democracy & Technology and eHealth Initiative & Foundation).

28. *AMA Privacy Principles* (American Medical Association).

About the Authors

Hadly Clark is an associate director at FasterCures who currently oversees our health data and technology portfolio of projects, and our oncology-related workstreams, including multi-cancer early detection. She is known for her expertise in health tech, quality and process improvement as well as product design, creating consumer portals and smartphone apps that empower patients. She has also served as a dedicated patient advocate, writing appeals, reviewing bills, requesting and collating records on behalf of patients. She received her graduate degree in health systems administration from Georgetown University with a focus on quality improvement and healthcare operations.

Jessica Marshall is an associate at FasterCures. In her role, she conducts daily in-depth research for the COVID-19 Vaccine and Treatment Tracker, contributes to ongoing health-equity issues occurring across the biomedical ecosystem, and facilitates the development of trust within the health technology and data sector. Prior to FasterCures, Marshall was a graduate fellow at the Veterans Health Administration, where she aided studies focused on identifying veteran groups experiencing health disparities in the US and building trust to advance veteran health equity and knowledge of the COVID-19 virus. She holds a BS in biochemistry from The George Washington University and a Master of Public Health in global health policy from the Milken Institute School of Public Health at The George Washington University.

SANTA MONICA | WASHINGTON | NEW YORK | LONDON | ABU DHABI | SINGAPORE