AMA
AMERICAN MEDICAL ASSOCIATION

PRIVACY IS GOOD BUSINESS

A case for privacy by design in app development

Summary

Our ability to collect and track health and wellness data in recent years has had positive benefits for a growing population of users across the United States. Physicians and care teams can more closely monitor known conditions and proactively engage with patients around their health concerns. Individuals can choose from a myriad of mobile applications ("apps") to manage their weight, monitor their blood sugar, access clinical and peer support for behavioral health, and much more. Researchers have access to more data that can be combined with socioeconomic and demographic information to aid in building predictive models or identify at-risk populations to improve access to and coordination of care. Federal regulation has also created pathways for individuals to download their medical records directly from their physician's electronic health records (EHR) onto one's smartphone.

However, as more data is collected and exchanged, there is often a lack of discussion around ensuring that individuals understand who is collecting that data, who they are sharing it with, what will be done with it, and whose responsibility it is to protect sensitive health data. This discussion is critical to advancing adoption of innovative health technologies, particularly if such technologies aim to improve health equity. Unfortunately, society is learning that greater access to digital heath information can have harmful consequences, whether intended or not. While none of us are safe from these risks, the impact can be particularly problematic when data is used to exclude or provide substandard care for those in historically marginalized communities. Examples abound. Health insurers have used information from wearable devices to deny claims for reimbursement, employers have used access to health information that employees may not be aware of to make employment decisions, and data brokers seek to collect more and more of this information to create in-depth profiles of individuals that serve as gatekeepers to opportunities for housing and more.

Through the development and release of its "Privacy Principles" in 2020, the American Medical Association seeks to provide guidelines for digital health data collection and equitable data governance. These guidelines aim to help technology developers navigate this space so that patients and clinicians can make informed choices about privacy. This paper seeks to help developers and implementers of mobile health apps put the Privacy Principles into action—strengthening patient and physician trust in those apps.

Introduction

The explosive growth of smartphone use, wearable fitness devices, and the ease by which apps can be built and integrated into the phones has made both receiving data and inputting data a norm in many consumers' daily habits. Users have grown accustomed to having the world at their fingertips via their phone. More and more, that world includes health-related data. As part of the recently rolled-out rules implementing the 21st Century Cures Act, patients also now have the right to access their own electronic health records directly from their physician's EHR system "in a form convenient for patients, such as making a patient's electronic health information more electronically accessible…."[1]

In today's environment—where bank accounts, work benefits and utilities records can be accessed via smartphone in seconds—users want and expect their health information to be just as convenient and safe to access. Consumers are also using apps to aid in tracking their own health, from blood pressure to weight and mood. Because patients are used to health care facilities protecting their data as required by the Health Insurance Portability and Accountability Act (or HIPAA, which is further defined below), app users may assume that much of the health information collected and stored in apps will be kept private. However, in reality, most of the apps they are using are not subject to the same kinds of health privacy regulations as those that cover physician and health insurance company systems. The rules around what app and technology developers can do with that information are minimal and not well-defined.

When the Health Insurance Portability and Accountability Act of 1996 came to be, the various kinds of electronic devices and applications that could be used to gather and house health information were limited and the future direction of such technology was not yet anticipated. Today, some patients incorrectly believe that all health information is protected from disclosure by HIPAA. However, only information collected by *covered entities* (such as clinicians and health plans) is subject to HIPAA rules requiring privacy and security safeguards. While subsequent legislation (such as the California Consumer Privacy Act) has attempted to address some privacy concerns for patients, more comprehensive data privacy rules have not been implemented at the federal level. In sum, while covered entities have obligations under HIPAA related to privacy and security of protected health information, there are many non-covered entities that collect and transmit that same data without restriction or specific requirements to protect it.

Physicians have an obligation—and typically, a desire—to help their patients maintain privacy of their health data and are wary of personally recommending apps or devices that may seek to exploit their patient's privacy. Clinicians look to trusted sources using guidelines specifically developed by their profession and seek to recommend apps that follow that guidance, such as the App Advisor from the American Psychiatric Association. Another trusted source is the American Medical Association. In 2020 the AMA published a set of privacy principles, which build on longstanding AMA policy developed by the physician members of its House of Delegates, to help guide the digital health information industry and regulators. The AMA's "Privacy Principles " were born from the idea that third parties accessing an individual's data should act as responsible stewards of that information. While some of the principles are legislative aspirations, the majority can be viewed as system guidance for app developers who want to adhere to the privacy ideal that preserving patient trust is critical.

Digital health apps and data privacy

The meteoric rise in smartphone use with 85% of U.S. consumers owning at least one smartphone[2] has also led to widespread availability of an array of consumer apps. These include apps that help users track and store health, fitness and wellness information. In additional to smartphone apps, at least 1 in 5 Americans use some kind of smart watch or wearable fitness tracker.[3] Consumers have become accustomed to having health and wellness information at their fingertips and they can count on over 300,000[4] different apps to aid them. The recent publication of the rules associated with the 21st Century Cures Act, mandating that consumers have access to their electronic health records, has opened a new class of apps that can accept uploads of patient records at the patient's direction, often outside of the umbrella of HIPAA. Patients are now seeking advice and recommendations from their physicians for apps to house their electronic medical records, and a recent Pew Survey[5] showed that 90% of respondents preferred apps pre-approved by their physician. Accordingly, there is an opportunity for physicians to place patient privacy at the center of this discussion and for app makers to distinguish their products from the competition by ensuring their products prioritize privacy.

Patients will be seeking advice and recommendations from their physicians for apps to house their electronic medical records, and a recent Pew Survey showed that 90% of respondents preferred apps pre-approved by their physician.

What does your business know about *your* business?

Health and wellness apps like period, pregnancy, and fitness trackers are gaining popularity in the workplace as they increasingly are promoted by companies in collaboration with their health insurance providers. Many employers offer employees the opportunity to participate in wellness programs that track participation in exchange for subsidies on health insurance premiums, monthly checks based on the number of steps walked, or other benefits. While the convenience of having a ready tracker for assistance in weight management, exercise, period tracking and conception planning may seem appealing, more and more of these apps have been collecting personal private details and sharing them with health insurers, employers, and data aggregators like Facebook and Google. A series of investigative articles by the *Washington Post* found that employers were paying to gain access to information input into period tracking apps and fitness trackers that were being promoted by the employer's health insurance company.[6] Both managers and human resources personnel had access to this information. Yet it's nearly impossible to ensure that such information is not used by employers to make arbitrary decisions about an employee's continued employment, salary, promotion potential and more. For example, employers receiving reports from insurers about their employees' daily number of steps could infer that less-active employees are costing the business more money in insurance premiums. Suddenly, employees with mobility limitations due to disability or chronic health conditions or those who live in unsafe neighborhoods may be at greater risk of losing their job, again demonstrating how a loss of data privacy can create or exacerbate inequities.

Using a digital weight management app as an example, the kind of data that is collected by the app may seem harmless to the user at first. A typical weight management app collects information like height, weight, body fat percentage, sleep times and patterns, caloric intake, types or even brands of foods eaten, exercise, and in some cases, mood, blood sugar and blood pressure. This kind of information may not seem like medical data when the user was entering it into the app, but as a picture of a person's health begins to evolve from the information submitted, it starts to look more and more like what might be found in a medical record. A marketer, an insurance company, or an employer could have access to that information and use it in ways that the consumer may not have imagined. Accordingly, apps can differentiate themselves by building trust with consumers that their personal private data will not be shared with unknown or unwanted parties.

As an example scenario, a person using a digital weight management app over six months faithfully might paint a picture of an individual at risk for type-2 diabetes, who is struggling to lose weight and perhaps has concerning blood pressure trends. This person dutifully enters all their meals and includes information like alcohol consumption. If the app was recommended to the user by their employer's benefits program (as many are today), is the information the user inputs going back to the employer? Depending on what the terms of use are for the app, the employer or even the employer's health insurance company may have access to that information.[6] Employees may be uncomfortable with their employer's knowledge of details of their dietary and alcohol consumption, which could lead to bias or outright discrimination that manifests through failure to provide merit-based promotions or raises, or even termination.

Employers are not the only entities that can use health data to make decisions about individuals. Health insurers accessing health-related data also use that data for health scoring and pricing.[7] For example, insurers and other third parties collect data from medical devices used at home—sometimes without the patient's knowledge or consent. Insurance companies have been found to deny claims for continuous positive airway pressure (CPAP) machine users when patients are not consistently using the device even if the patient is not using it for legitimate reasons (e.g., a mask not fitting properly).[8] Today's CPAP machines are sending usage information not only to insurers but also to the machine manufacturer's and even the medical supply companies providing the machines and accessories.[8] This sharing of data is allowed under current federal privacy laws.

"The companies are tracking your race, education level, TV habits, marital status, net worth. They're collecting what you post on social media, whether you're behind on your bills, what you order online. Then they feed this information into complicated computer algorithms that spit out predictions about how much your health care could cost them."

Marshall Allen, health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates, NPR and ProPublica, July 17, 2018

The harms perpetuated by unrestricted data sharing are not limited to health or employment and have the potential to actually exclude individuals from opportunities to better their lives. In 2016, the Federal Trade Commission (FTC), a federal agency charged with a range of consumer protection activities, released its report, "Big Data: A Tool for Inclusion or Exclusion?" to explore the potential of big data both to create opportunities for consumers and to exclude them from such opportunities.[9] The report was based on the types of data provided through consumer-facing apps, such as those described above. Unsurprisingly, the report found that big data offers vast possibilities for both help and harm. Specifically, it noted that big data has the potential to target educational, credit, health care, and employment opportunities to communities with low income and under-resourced populations. At the same time, however, the report states that potential inaccuracies and biases might lead to detrimental effects for the very same populations.

Unfortunately, in the time since the report was published, we've seen examples of how such biases limit opportunities for marginalized populations. The vast amounts of data that we produce—and which are aggregated, sliced, and diced by third parties—has facilitated the development of risk scores by a wide range of companies, including health insurers.[10] Most people are not even aware these scores exist.

These types of unchecked data processing and algorithmic decision-making practices can amplify discrimination based on race, gender, sexual orientation, ability, age, financial status and other group membership. For example, in March of 2019, the U.S. Department of Housing and Urban Development (HUD) sued Facebook for "encouraging, enabling and causing housing discrimination" when it allows companies that use the platform to improperly shield who can see certain housing ads.[11] HUD also alleged that "Facebook allowed advertisers certain tools on their advertising platform that could exclude people who were classified as 'non-American-born,' 'non-Christian' or 'interested in Hispanic culture,' among other things."[11] It also said advertisers could exclude people based on ZIP code, essentially "drawing a red line around those neighborhoods on a map"[11]—a digital translation of the redlining policies that have oppressed marginalized populations across the United States historically, particularly throughout the 1900s. These types of practices are only more harmful when combined with sensitive health information. More must be done to help people protect themselves from the misuse and abuse of their data.

"The vast amounts of data that we produce—and which are aggregated, sliced, and diced by third parties—has facilitated the development of risk scores by a wide range of companies, including health insurers. Most people are not even aware these scores exist."

Consumer consent must be meaningful

The digital health information collected by wellness apps or wearable devices and shared among data brokers, insurance companies or even social media companies like Facebook may not worry consumers who are used to sharing many aspects of their lives in today's digital culture. However, once that data is out there, it's almost impossible to re-bottle. Furthermore, organizations you interact with may use your information as a basis for making decisions that may be against your best interests—such as decisions around whether you and your children can obtain life insurance, and restrictions on coverage amounts when you apply for a health insurance plan or seek to use its benefits.

Additionally, consumers are largely unaware of all the ways their data is collected and shared. Users are finding out after-the-fact that certain companies have been collecting and sharing their data in ways they didn't envision, such as merging wellness data with available personal genomic data that was also voluntarily given away via a direct-to-consumer genealogy service.[12] For example, the Facebook SDK (Software Development Kit) is a common way for apps to collect user data, ultimately sending it to Facebook for uses like targeting advertising, without the user knowing that data is being collected and shared.[13] SDKs are a common way for developers to add functions to their apps that they don't want to build on their own, but many share user data with their originating system, meaning that unknown third parties may have access to user information in ways perhaps even the app developer was not aware of. Consumers are not comfortable with these practices and are overwhelmingly in favor of companies being more proactive about data privacy. A study by PWC shows that over 90% of consumers agreed that companies should be responsible for ensuring data is safe and used responsibly.[14]

I saw it on Facebook

The rise in direct-to-consumer apps that can obtain and house consumer health information without being subject to HIPAA regulations is growing. Consumers may be unaware that the health information they upload to an app is no more protected from disclosure to third parties than any other type of app data. This can include sensitive health records requested by the consumer and uploaded from an EHR to an app on their smartphone. (BMJ, 2021)

Health and fitness apps are already known to share users' data directly with Facebook or other data collectors, unbeknownst to the consumer and even when the consumer does not have a Facebook account. Consumers may not be aware that information like heart rate, weight, height or even mental health concerns may be funneled by that app to Facebook via the Facebook SDK. This is called "Off-Facebook Activity" and is a growing trend in the data collection space.

(Schechner & Secada, Feb. 22, 2019)

Another category of apps that has grown tremendously in the last few years is addiction and recovery assistance apps. Again, using SDKs from companies like Facebook, Zoom and Google, the app developers are knowingly or unknowingly exposing some of the user's data to third parties, including ad generators and data aggregators. Users may be unaware that data related to their substance abuse treatment is shared with strangers for unknown purposes.

(Morrison, July 12, 2021)

Some app and wearable device companies have mechanisms to collect consent for data sharing and most advertise their data sharing practices in their "Terms of Service." All too often consumers bypass reading the lengthy and confusing legal text of such agreements and/or misunderstand what they have agreed to in their consent. Often, the consent controls and privacy policies are not clear or specific enough to be meaningful to consumers. By providing clear consent controls and easy-to-understand terms of service, these companies can take proactive steps toward becoming responsible stewards of health and wellness information while promoting equity by ensuring all users can understand the app's data practices and take advantage of its privacy controls.

Balancing user wants with ethical privacy practices

Physicians understand that patient health data is both useful and powerful. That said, personal health information getting into the wrong hands or being used to deny patient treatment or make obtaining treatment more difficult is a risk in today's digital landscape. As a partner to physicians for over 170 years, the AMA is a trusted source for clinicians looking for guidance on what makes for good privacy practices. Physicians may be more willing to make app recommendations to their patients if they know those apps and wearable devices follow a comprehensive set of privacy guidelines created by a professional physician or medical association and focused on protecting the trust at the heart of the patient-physician relationship.

Physicians may be more willing to make app recommendations to their patients if they know those apps and wearable devices follow a trusted set of privacy guidelines created by their industry for their industry.

As discussed in this paper, investigative reports are increasingly showing how various entities use health-related data along with other demographic and lifestyle information to set health care prices, limit coverage, or withhold opportunities from certain individuals and communities. This practice frequently targets communities that already face disparities in health care outcomes due to systemic discrimination and that have fewer resources to advocate for their health care. There is also a growing concern that patients eager to manage the exchange of their health care data may opt to upload their digitally available health care information to apps despite misunderstanding that app's terms of service, which allow the app to share that information with unknown third parties. Despite the great promise of consumer-directed heath exchange allowing users to more easily obtain and share their medical records, portable medical records in the hands of unscrupulous businesses or data brokers is a wild-west scenario that is just beginning to play out in the United States.

As it becomes clearer how much of a consumer's personal information, including health information, is being shared with companies like Facebook and Google, apps with a reputation for privacy-by-design will find themselves in a strong position with consumers and physicians—and, potentially, regulators.

App and wearable device makers who choose to follow privacy guidelines as outlined by organizations like the AMA may have a strategic advantage with consumers concerned about digital privacy and with clinicians making recommendations to patients. A survey by Black Book found that 57% of health care consumers are concerned about health IT and data privacy concerns, noting that such concerns often prevent them from sharing certain health data with their doctors.[15] In this regard, continued industry failure to prioritize privacy in technology could have significant implications for patient safety.

As it becomes clearer how much of a consumer's personal information, including health information, is being shared with companies like Facebook and Google, apps with a reputation for privacy-by-design will find themselves in a strong position with consumers and physicians—and, potentially, regulators. Federal and state legislators are increasingly introducing and enacting more comprehensive digital privacy laws, such as the California Consumer Privacy Act. Additionally, the FTC has clarified to the industry that apps (including those connecting to EHRs via application programming interfaces, or APIs) are subject to its Health Breach Notification rule and accompanying—and poised to increase—enforcement efforts.[16] Businesses that deal in personal information have choices to make in terms of *privacy debt*; is it easier to implement good data privacy now or scramble to meet privacy regulation and data clean up later?

AMA privacy principles: A checklist for app developers

The AMA's "Privacy Principles" consider privacy policy from several angles, including individual rights, equity, entity responsibility, legislation and enforcement. The following checklist, which pulls privacy principles from the "Individual Rights," "Equity" and "Entity Responsibility" sections of the document, denotes several specific actions developers can take to implement the principles. They are meant as guidelines for businesses that deal with digital health and wellness information, and that want to follow trusted guidelines for collecting, storing and sharing patient health data. Adopting these guidelines can help bolster understanding of and trust in your company's data privacy practices—an important move that can make your apps more appealing to patients and physicians.

Individual Rights	
Privacy Principle	**Action**
1. Individuals have the right to know exactly what data of theirs an entity is accessing, using, disclosing, and processing—and for what purpose—at or before the point of collection.	**1.1** Systems shall identify the intended purpose(s) for all data processing for each entity that might have access to their personal data.
	1.2 Systems shall identify all data an entity is accessing, using, disclosing, and processing and the intended purpose prior to the point of collection.
	1.3 Systems shall log all access to personal data.
	1.4 Systems shall provide the ability to review personal data access logging information to the user that owns the personal data.
2. Individuals have the right to control how entities access, use, process, and disclose their data, including secondary (and beyond) uses.	**2.1** Systems shall provide configurable settings functions to allow the user to define which entities may have access to their personal data.
	2.2 Systems shall identify the mechanisms by which individuals may control how entities access, use, process, and disclose their data, including secondary (and beyond) uses.
	2.3 Systems shall identify all entities with the ability to access personal data, the purpose of data sharing, and whether or not personal data is sold and for what purposes.

Privacy Principle	Action
	2.4 Systems shall deny access to a user's personal data if the entity is not identified in a configurable setting function that allows the user to set or deny access.
	2.5 Systems shall ensure that control setting information and methods comply with ADA, Section 508 for accessibility.
3. Individuals should be notified within a reasonable period of time following a material change in the entity's data access, use, disclosure, and processing practices.	**3.1** Systems shall provide an initial notification, as defined in the end user license agreement, number of days prior to any material change to an entity's data access.
	3.2 Systems shall identify notification agreements (including time to notification from change) related to material changes in the entity's data access, use, disclosure, and processing practices.
4. Individuals have a right to direct entities not to sell or otherwise share data about them.	**4.1** Systems shall provide a configurable setting function to allow a user to set whether or not their personal data can be sold or otherwise shared.
	4.2 Systems shall identify which settings are available and the function of those settings in relation to the sale or sharing of personal data.
	4.3 The default setting of an application should be to deny sale of a user's personal data, with a requirement for a user to opt-in explicitly.
5. Individuals and entities should be able to protect and securely share pieces of information on a granular, as opposed to a document, level.	**5.1** Systems shall provide a configurable setting for each category of personal information that can be potentially shared.
	5.2 Systems shall identify which categories of personal information can be controlled through configurable settings.
6. Individuals have a right to direct an entity to delete their data across the entity's ecosystem of services, including when the entity goes out of business or is bought out by another entity (with potential narrowly delineated exceptions, as determined by regulatory bodies and consistent with stakeholder input).	**6.1** Systems shall provide a configurable setting to direct the deletion of all personal data from an application and entities authorized for data sharing. This includes options for directing the deletion of data from the device and data stored outside of the device (such as cloud storage).
	6.2 Systems shall identify the mechanisms and policies related to the individual's right to direct deletion of all personal data from an application.
	6.3 Systems shall identify the mechanisms and policies related to the individual's right to direct deletion of all personal data from a specific entity authorized for data sharing.
	6.4 Systems shall direct the deletion of all user personal data from an application and entities authorized for data sharing upon going out of business.
7. Individuals have the right to access and extract their data from a platform in a machine-readable format.	**7.1** Systems shall provide a user with the ability to extract their personal data for review in a common machine-readable and non-proprietary format.
	7.2 Systems shall identify the mechanism(s) available to the individual to extract their personal data.

Privacy Principle	Action
8. Individuals should have the right to know whether their data will be used to develop and/or train machines or algorithms. The opportunity to participate in data collection for these purposes must be on an opt-in basis.	**8.1** Systems shall make the consent for participation in data collection for use in developing and/or training machines or algorithms a configurable setting. The settings shall require the user to explicitly opt-in for data collection for this purpose.
	8.2 Systems shall deny data collection of a user's personal data by default unless the user has changed their configurable setting to allow it.
	8.3 Systems shall depersonalize any data used to develop and/or train machines or algorithms and communicate depersonalization practices to users.
9. Privacy rights should be honored unless they are waived by an individual in a meaningful way, the information is appropriately de-identified (using techniques that are demonstrably robust, scalable, transparent, and provable), or in rare instances when strong countervailing interests in public health or safety justify invasions of privacy or breaches of confidentiality and, in such case, to the minimum extent necessary.	**9.1** Systems shall identify agreed upon terms for honoring privacy rights unless they are waived related to information de-identification or in rare instances when strong countervailing interests in public health or safety justify invasions of privacy or breaches of confidentiality and, in such case, to the minimum extent necessary.
10. Disclosures of an individual's data should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure.	**10.1** Systems shall limit disclosure of personal data elements to only those elements needed to fulfill the immediate and specific purpose requested. For example, an app housing medical record data shall not disclose information like user geolocation.
11. Individuals who access their medical records using apps should have mechanisms to annotate—but not change—the copy of the record they hold. These mechanisms should track who made the annotation, when, how, and why.	**11.1** Systems shall provide annotation functionality for users to have the capability to annotate copies of their records.
	11.2 Systems shall identify the annotation functionality available for annotate copies of the records held while indicating that such notes shall not change the data.
	11.3 Systems shall maintain an annotation history for all users that make annotations to copies of a user's record.
	11.4 Systems shall identify what and how annotation history for users that make annotations shall persist in the system.

Equity	
Privacy Principle	**Action**
1. Privacy protections should promote equity and justice.	**1.1** Systems shall implement privacy protections that recognize barriers to equity and work to create an equal access and opportunity for all users.
	1.2 Systems shall implement privacy protections that are fair and reasonable regardless of user.
2. Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as "sensitive" or protected health information under HIPAA—and individuals accessing, processing, selling, and using it without the individual's best interest at heart can cause irreparable harm.	**2.1** Systems shall treat all user health care information with the same regard for privacy regardless of whether it is legally defined as sensitive or protected under HIPAA.
3 . Individuals should be protected 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. Similarly, individuals should be protected from discrimination, stigmatization, profiling, and exploitation based on inferences drawn from a refusal to use or cessation of use of an app or digital health tool.	**3.1** Systems shall protect consumers from discrimination, stigmatization, discriminatory profiling, and exploitation as part of the collection and processing of health care and related data.
	3.2 Systems shall protect consumers from discrimination, stigmatization, discriminatory profiling, and exploitation resulting from the use and sharing of health care and related data.
	3.3 Systems shall protect consumers from discrimination, stigmatization, discriminatory profiling, and exploitation with an equitable application of protection and ensure that users from historically marginalized communities, e.g., people without housing, people with disabilities, LGBTQ+ people are afforded the same protections.
	3.4 Systems shall protect consumers from discrimination, stigmatization, discriminatory profiling, and exploitation based on their choices related to data sharing, refusal to share, or cessation of use of an application or digital health tool.
	3.5 System shall provide the same level of functionality for all users regardless of permissible use selections.
4. Because low-income individuals and other vulnerable populations have fewer resources and tools at their disposal to effectively assert their privacy rights, purchase technology with the most advanced and up-to-date privacy and security technology, and recover from harmful invasions of privacy, privacy frameworks (legal or otherwise) must advance policies to benefit individuals of all income levels. For example, the AMA would not support a policy in which paid apps provided greater privacy protections than free apps.	**4.1** Systems shall consider equity in relationship to an individual's ability to purchase technology, recover from privacy breaches, or advocate for their privacy rights effectively.
	4.2 Systems shall not make protections of privacy greater in applications or digital health tools based on fees for service or technology selections made by a consumer.

Privacy Principle	Action
5. Law enforcement agencies requesting medical information should be given access to such information only with a court order and if the law enforcement entity has shown, by clear and convincing evidence, that the information sought is necessary to a specific, legitimate law enforcement inquiry; that the needs of the law enforcement authority cannot be satisfied by nonidentifiable health information or by any other information; and that the law enforcement need for the information outweighs the privacy interest of the individual to whom the information pertains. Any applicable legal requirements for law enforcement access to medical information imposed by federal, state, or local laws shall apply in addition to this principle.	**5.1** Systems shall pledge to only provide identifiable health care data to law enforcement either due to court order and if the law enforcement entity has shown by clear and convincing evidence that the information is necessary to a specific and legitimate law enforcement inquiry and that the law enforcement need for the information outweighs the privacy interest of the individual to whom to information pertains.
	5.2 Systems shall adhere to all applicable federal, state, and local laws when responding to requests for access to medical information from law enforcement.
6. Employers and insurers should be barred from unconsented access to identifiable medical information to assure that knowledge of sensitive facts does not form the basis of adverse decisions against individuals, such as non-coverage of stigmatized health conditions.	**6.1** Systems shall deny employers and insurers from unconsented access to identifiable medication information.
	6.2 Systems shall prevent use of consented or unconsented accessed medical information from being used to form the basis of adverse decisions against individuals.

Entity Responsibility

Privacy Principle	Action
1. All entities that maintain an individual's health information should have an obligation or "duty of loyalty" to the individual, including the duty to maintain the confidentiality of that information.	**1.1** Entities shall maintain an individual's health information confidentially; employing policies and procedures that protect the consumer over all other considerations.
2. An entity must disclose to individuals exactly what data it is collecting and the purpose for its collection. Such information should not be used for a materially different purpose than those disclosed in the notice at the point of collection of such information. For example, an entity that collects location data to provide weather should not use that data for advertising.	**2.1** Entities shall disclose to individuals exactly what data it is collecting prior to or at the point of collection.
	2.2 Entities shall disclose to individuals exactly the purpose is for all data collected prior to or at the point of collection.
	2.3 Entities shall not use information collected for a purpose that is materially different than the purpose disclosed in the notice at the point of collection of such data.

Privacy Principle	Action
3. Entities should only collect the minimum amount of information needed for a particular purpose, in accordance with regulation and/or federal guidance. For example, a weather app may need general location data (e.g., ZIP code), but not precise location data (e.g., GPS coordinates).	**3.1** Entities shall not collect more than the minimum necessary data needed for a particular purpose.
4. Entities should establish and make publicly available a data retention policy with established protocols for retaining information for operational or regulatory compliance needs.	**4.1** Entities shall publicly disclose their data retention policy, including details related to established protocols for retaining information for operational or regulatory compliance needs.
5. Entities should be required to disclose to individuals what specific elements of data they collect, why, how often, for what purpose, and specifically with whom they are sharing the data.	**5.1** Entities shall disclose to individuals which specific data elements and data categories they collect. The description of such data elements and/or categories should be able to be easily understood by individuals with low literacy skills.
	5.2 Entities shall disclose to individuals the purpose of the data elements they are collecting. (Note: "purpose" and "why" are the same here.)
	5.3 Entities shall disclose to individuals how often they will collect data elements.
	5.4 Entities shall disclose with whom they are sharing data they collect.
6. Privacy policies should be written to promote understanding by individuals with elementary school levels of reading comprehension. Terms should be clearly defined and unambiguous. For example, statements such as, "We may share this data with our partners to improve quality" are vague and should not be permitted.	**6.1** Entities shall explain terms and conditions of app or digital health tool use in plain language that is able to be read and understood by individuals with low literacy skills and/or individuals of diverse cultures and language.
7. Entities should be prohibited from using health data to discriminate against individuals, including creation of "risk scores" that could hinder patients and their families from receiving health, disability, or life insurance; housing; employment; or access to other social services.	**7.1** Entities shall not use health data to aid or abet discrimination or the ability to access products and services for an individual or their family.
8. Entities should make their de-identification processes and techniques publicly available.	**8.1** Entities shall publicly disclose their data de-identification processes and techniques.

Endnotes

1. I.A Executive Summary, Purpose of Regulatory Action, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Health and Human Services, May 1, 2020
2. Pew Research, April 7, 2021
3. Emily Vogels, Pew Research, Jan. 9, 2020
4. The Growing Value of Digital Health, IQVIA Institute, November 2017
5. Americans Want Federal Government to Make Sharing Electronic Health Data Easier, Pew Trusts, Sept. 16, 2020
6. Christopher Rowland, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, *The Washington Post*, Feb. 16, 2019
7. Marshall Allen, Health Insurers Tap Data Brokers To Help Predict Costs, NPR, July 17, 2018
8. Marshall Allen, You Snooze, You Lose: How Insurers Dodge the Costs of Popular Sleep Apnea Devices, NPR, Nov. 21, 2018
9. Big Data, a Tool for Inclusion or Exclusion?, FTC, February 2016
10. Pam Dixon and Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, World Privacy Forum, April 2, 2014.
11. Tracy Jan and Elizabeth Dwoskin, HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe, Washington Post, March 28, 2019.
12. Marshall Allen, Health Insurers Tap Data Brokers To Help Predict Costs, NPR, July 17, 2018
13. Megha Rajagopalan, Maya and MIA Fem Are Sharing Deeply Personal Data With Facebook, Buzzfeed News, Sept. 9, 2019
14. PWC, Consumer Intelligence Series: Protect.me, PWC, 2017
15. Sara Heath, Privacy Issues, Distrust Keep Patients from Health IT Engagement, xtelligent Heathcare Media, Jan. 3, 2017
16. FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule, Sept.15, 2021

Resources

- You Give Apps Sensitive Personal Information. Then They Tell Facebook, *The Wall Street Journal*, Feb. 22, 2019
- The struggle to make health apps truly private, Vox, July 12, 2021
- AMA Privacy Principles, an American Medical Association resource
- CCPA, California Consumer Privacy Act
- 21st Century Cures Act, a Department of Health and Human Services resource
- HIPAA, Health Insurance Portability and Accountability Act resource from the CDC
- APA App Advisor, an American Psychiatric Association resource
- HITECH Act, Federal Register resource