Chapter 10
Healthcare Privacy

Vivian Genaro Motti and Shlomo Berkovsky

Abstract As healthcare shifts towards the digital realm and healthcare delivery steers to patient-centric solutions, new privacy risks emerge. Such risks are acknowledged, but understanding and addressing them with privacy-enhanced technologies is practically challenging. This chapter describes privacy concerns and risks that emerge with the digitization of healthcare services, the availability of Internet-of-care-things, and the usage of online services for medical data. To ensure patients' privacy, collaborative efforts from stakeholders are necessary. Patients, practitioners, and family members play an important role, along with medical organizations, including hospitals, insurance companies, and clinics. Privacy-preserving mechanisms go beyond the protection of patients' data to the infrastructure of medical devices, networks, and systems. The data life cycle, from collection to disposal, must be considered when implementing privacy protections. Principles, policies, and regulations addressing privacy are limited and costly to implement, failing to cover novel technologies that collect and transmit medical data. In the USA, HIPAA is the de facto policy standard. Nevertheless, HIPAA disregards data collected by wearable sensors, fitness trackers, and smartwatches. It does not consider social media networks, mobile applications, and discussion forums where users share medical information. Lastly, genetic data available through online profiles rises privacy issues that are neither known nor regulated.

V. G. Motti (✉)
George Mason University, Fairfax, VA, USA
e-mail: vmotti@gmu.edu

S. Berkovsky
Macquarie University, Sydney, Australia
e-mail: shlomo.berkovsky@mq.edu.au

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_10

10.1 Privacy in Healthcare

Privacy considerations for medical records aim at protecting patients and their data by preventing unauthorized access to personal health data by third parties [49]. To ensure privacy, access control mechanisms enforce authorized access to protected patient information. The goal of privacy in this case is to ensure that the patients' information is protected while facilitating the provision of healthcare services. Thus, privacy controls should be incorporated to prevent data misuse and exploitation as well as abusive and discriminatory practices. For instance, they can block a health insurance company from denying care or raising healthcare costs to a patient, or prevent an employer discriminating job applicants, who are more likely to become sick or disabled.

Privacy concerns are important regardless of the industry sector at stake or the profile of the user involved. Still, certain users may be more vulnerable to privacy risks, due to their limited awareness of threats or limited understanding of the intricate details of the technology. Specifically, users with cognitive impairments [1] and older adults may face higher risks due to quick technological changes and challenges to follow and understand updates in business models [2, 51]. They are also subject to remote monitoring by caregivers and practitioners [3], for instance, with self-trackers, robots, or smart home technologies that support older adults' ability to age in place [4, 5]. The continuous use of technology in such cases exacerbates risks and may result in flawed controls for data access [6].

Self-tracking afficionados may also be vulnerable due to the risk of unintended exposure of their data, since their data is collected continuously, from various sources, and can be aggregated by online services, such as social media channels [7]. Self-tracking has become even more popular due to the COVID-19 pandemic, allowing users to monitor their vital signs, helping government authorities to surveil citizens' mobility and trace their contacts, to monitor the spread of the disease. The proliferation of contact tracing applications led to important discussions regarding the extent to which state controls and federal regulations can impact the citizens' rights to privacy. While technology can help address the pandemic, it is unclear how to optimize its use for common benefits in a fair manner [8].

In addition to the user profile and the purposes of technology, several aspects of how data flows are also important when building effective privacy controls for digital records. This includes considering privacy controls for the data sources and systems used to process medical data [44]. Moreover, it is important to consider the devices, equipment, stakeholders, and processes employed seeking to identify privacy risks and protect user data.

First, the data sources that could pose privacy risks include systems and applications that manage protected medical data. Beyond dedicated systems used by health providers, consider also various devices and systems used by patients. These include websites, discussion forums, mobile applications, and social media channels. While some of these have medical focus, many are rather general-purpose systems employed by users to learn about medical content, exchange information

with others, track health conditions, and post or discuss questions with a virtual community [48, 55].

Next, all the equipment used for data collection or processing needs to have the right privacy protections, as both physical and virtual artifacts require privacy controls. To protect these assets, a thorough risk analysis should be conducted. The duration and costs associated with such an analysis depend on the scale of the system. Generally, such analyses range from an informal internal assessment to detect potential risks to a systematic procedure carried out by a specialized service with a team of domain experts. Either way, the purpose of the analysis is to identify and mitigate vulnerabilities and breaches at the software, hardware, or operational process level.

Physical equipment that may need to be protected includes wires, ports, and drivers. While locks, latches, and keys facilitate physical safeguards, virtual applications and software, on the other hand, demand specialized systems. These include firmware and tools deployed to monitor the use of assets and control access by end users, third parties, or virtual agents. Compliance with standards and policies helps regulating access by third-party systems or external services, including cloud solutions for platforms, infrastructure, and software.

Although the patient is the main beneficiary of privacy considerations in healthcare, collaborative efforts from *multiple stakeholders* are necessary to prevent unintended disclosure and malicious use of personal data. As diverse stakeholders are involved in the data generation, analysis, and interpretation, they should be trained and qualified to manage health information with adequate privacy-preserving behaviors and attitudes. Medical practitioners, caregivers, family members, investigators, and organizations all need to take responsibility for protecting patient data from unwanted disclosure and access. Additionally, health insurance companies, clinics, pharmaceutics, and laboratories also need to actively preserve patient privacy.

To ensure users' privacy is preserved, consider different data types, information sources, and stakeholders in the entire life cycle. Data protection requires an integrative approach combining *multiple strategies* ranging from training users to deploying and testing technical controls. The training aims at raising privacy awareness, educating and informing end users about adequate behaviors when using data, equipment, systems, and resources. Technical controls aim at protecting all the assets involved and include authentication, authorization, protected network connections, obfuscation and firewalls [43].

Multiple data sources need to be considered when designing for privacy in healthcare. This includes reports written by healthcare practitioners (prescriptions of medication and therapies), caregivers (checklists and documentation), or patients (self-assessment reports and receipts). This also includes data collected in a passive or active way, from applications that use ambient sensors, to mobile applications where users report data [2, 50]. Data in various formats and modalities should be governed by privacy control mechanisms, be it imaging and signals from clinical examinations and text reports or raw data generated during clinical examinations with medical devices. Aggregated data from a patient's electronic health records (EHRs) should also be protected.

When implementing privacy controls for healthcare, concrete *artifacts* for consideration include EHRs, medical reports, notes, and prescriptions. However, not all medical data comes from health records, as information can be inferred from the user's location, lifestyle, and behaviors, among others [10]. The digital phenotype of patients can be defined based on their online behaviors, e.g., search history and social media posts [9]. On the one hand, these offer valuable information about patients' lifestyle, health status, well-being, and future condition [11]. On the other hand, this information poses new privacy risks, especially when the user-generated content becomes publicly available. Furthermore, the potential for inferences on public data increases when multiple data sources are aggregated, leading to a greater risk of identifying sensitive data, including the address, social circles, and more.

From a technical perspective, the entire system infrastructure must be considered to ensure holistic privacy controls. As Fig. 10.1 illustrates, this infrastructure is centered on the patient, but includes the devices and equipment, where data is collected, stored, or shared, like sensors, browsers, mobile applications/devices, and computers [46]. Servers, databases, hard drives, and cloud services exemplify

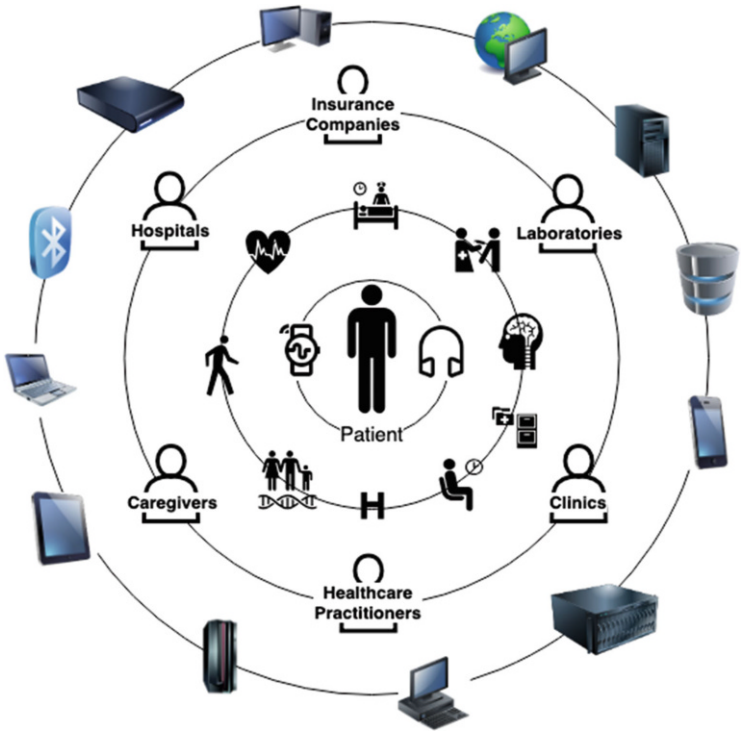

Fig. 10.1 To protect health data, privacy solutions should employ a holistic patient-centric approach considering the ecosystem of devices, data sources, and stakeholders involved in the process

applications and devices for storage purposes. Finally, network and communication protocols for exchanging information serve for data sharing and transmission.

Hardware and software solutions are part of the ecosystem for privacy-enhanced technologies. Electronic equipment, medical devices, mobile apps, and wearable technologies can be targeted when data access and sharing are enabled, posing privacy risks. The connection to the Internet exacerbates privacy risks, and special attention is needed when devices are integrated with third-party services. *Multiple stakeholders* are involved in the process of data collection, retrieval, and analysis. These are important assets for privacy considerations and include health practitioners (doctors, nurses, physicians, clinicians), service providers (therapists, dentists, caregivers), family members (relatives, guardians), and others.

In practice, examples of misuse of private data have been publicized in popular media, particularly involving private information that users were unaware of or unwilling to disclose, revealed by data analytics. A notorious case includes the 2012 "pregnancy prediction score" by Target that used the history of items purchased by a client to tailor advertisements. Targeted ads and coupons related to pregnancy and baby items were sent to a teenager. Initially, the father of the teenager complained about the incident, fearing that the advertisement could serve as a teenage pregnancy incentive. Later on, he apologized about the complaint since he realized the store had made a correct prediction about his daughter's pregnancy before it was actually disclosed [12]. Another example is the exploitation of mobile apps that track menstrual cycle of employees [47]. As reported by the press, data from the app was shared with the employer under the banner of "corporate wellness," practically revealing sensitive information about the employees' intimate lives. Even if the app usage is deemed voluntary and the data is shared in an aggregated way, there is a potential for privacy breaches related to discriminatory and abusive practices.

Genetic information publicized online thanks to the dissemination of DNA kits have become an increasing privacy concern as well. More specifically, privacy concerns emerged when genealogy findings about biological parents and abuse in fertility clinics were discovered [59]. Such genetic services can reveal confidential information to costumers through online genetic profiles, provided by services such as 23andMe and their data analysis [13, 14].

To provide definitions and concrete examples of healthcare privacy, this chapter is organized as follows. Section 10.2 illustrates the risks involved with protected health data, covering diverse information sources and the risks users face. Section 10.3 focuses on existing solutions, listing and describing the policies, principles, and regulatory tools. Section 10.4 discusses the limitations of existing approaches, presenting open questions for future research and development. Finally, Sect. 10.5 summarizes how healthcare privacy is currently managed and provides key recommendations for stakeholders.

10.2 Risks

As more patients have access to advanced healthcare services, not only more documentation from lab tests and examination results are generated, but also privacy breaches increase in risks and severity. The larger number of privacy risks can be attributed to several reasons. First, the increasing number of devices facilitates a large-scale data collection. Data collected more frequently and more continuously covers multiple information channels generating datasets are larger and have a higher inference potential with aggregated data sources. Second, interconnected devices for data collection and analysis require advanced controls to prevent unauthorized access to and inappropriate use of data. Such controls are relevant as the data is transmitted or stored, so access to storage services needs to include physical and virtual implementations. Third, current regulations and practices are insufficient for holistic privacy-preserving controls, as emerging problems are still unknown and often addressed reactively. In addition, public data analyzed at an aggregated level can lead to inference of sensitive information. An aggregated analysis, fusing data on user behavior, eating habits, and shopping, for instance, can surface valuable information about their health condition and potential illnesses, resulting in information unbeknownst to users [42, 54].

Lastly, the implementation of effective privacy controls is not trivial [3], especially when multiple data sources and stakeholders are involved, and potential problems are neither well understood nor formally characterized. Best practices, heuristics, and guidelines are often limited or lacking, tend to be complex, and costly to implement. The above challenges leave users with vulnerable systems and imminent risks of breaches. Issues in healthcare privacy include data misuse, breaches, threats, and other implications. Main risks are associated with access by unauthorized parties, inappropriate use, abuse, disclosure, or even unauthorized recording of medical data. Privacy implications affect medical data in multiple dimensions from the data to the service levels.

10.2.1 Data, Protected Health Information, and Applications

Medical records require protection against inappropriate access to prevent unauthorized access to personally identifiable, confidential, and sensitive patient information, such as address, social security number, chronic illnesses, disabilities, or diagnosed diseases. In the USA, the federal law Health Insurance Portability and Accountability Act establishes limits on health data access to protect medical data [11]. The implementation of strict controls is needed to ensure that, from a system level, the exchange of information follows appropriate policies [45, 52, 53]. Effective access control mechanisms use policies to preserve users' privacy by matching information and datasets according to the users' profiles and respective privileges. Such controls need to operate seamlessly across different

medical applications, including medical imaging systems, genetic tests, and online consultations. Additionally, they need to be updated regularly to evolve as the technology advances.

10.2.2 Sources and Stakeholders

Laboratories, health providers, and clinics are considered trusted parties for health services. As the data they provide are essential to the delivery of patient care, these parties need to comply with regulations, best practices, and existing policies that govern the access control and storage practices for medical data.

Regarding online sources and public domains, when patients provide self-reported information in discussion forums, online groups, and social media posts [15], they reveal private information. While some users deliberately advocate for their conditions and become a public reference for their communities, others prefer to remain anonymous. However, oftentimes they are oblivious to and unaware of potential implications of leaving permanent digital traces, as once the information is disclosed it may be used in the future against them, for instance, in discriminatory practices related to insurance premiums or employment opportunities.

For healthcare practitioners and medical experts, online health networks are valuable for disseminating information among team members in hospitals or during epidemy outbreaks [16]. Despite users being mostly unaware of or unconcerned about potential risks [17], once the data is published online, it is impractical to control its dissemination. The risks involved are even higher when vulnerable populations are at stake (see Chap. 15), for instance, with parents sharing information about children [18] or caregivers sharing information about patients with disabilities.

Also, when multiple sources of information from different online channels are used, data can be aggregated for inference, leading to higher risks of unveiling sensitive information. If a patient posts comments and questions about their symptoms in online forums, seeking for advice from the community in a non-anonymous way, this information can be used for diagnostic purposes and also misused afterwards to potentially disadvantage the patient. This is especially risky when accounts are linked across platforms, which may lead to the unintentional disclosure of anonymized data and information. Moreover, the analysis of the user discourse has the potential to reveal age, gender, location, and medical conditions. Examples of medical topics posted in such channels include mental illnesses [11, 19], nutrition habits [9], disabilities [20], and syndromes [3]. An example of discriminatory practice and surveillance related to public posts on social media concerns the government proposal to use social media posts to detect fraud in disability payments. Not only it is unfeasible to verify whether a person is disabled from an online picture or post, but the proposal also raised questions about the legitimacy and reliability of social media posts, but the proposal also raised questions about the legitimacy and reliability of social media posts, as well as about abusive behaviors related to online contents that could harm individuals' rights to privacy [21].

Online communities and discussion forums often contain sensitive health information [15]. Although patients share information to exchange their experiences and seek for advice, they may be unaware of potential risks and misuse of the disclosed data. In these communities, nicknames are used to mask the actual identities. However, depending on the nature of the questions and answers posted, sensitive information and personally identifiable data may become inadvertently available. As Fig. 10.2 shows, PatientsLikeMe provides simple language privacy specifications that allow users to see, change, or delete their data. They can also be notified if data is stolen and request the company to stop processing their data. Notably, PatientsLikeMe does not warrant the authenticity of any user's identity or data provided by them.

Mobile health applications also pose novel privacy risks in healthcare. When users install and use an app, their personal information is often tracked, combining passive sensing (e.g., navigation and call history, location, activities) with self-reported data. As there is no legislation to regulate the usage of such data [16], there is much space for exploitative practices. For instance, the Ovia Health app has been used as a monitoring tool to track intimate fertility and pregnancy information of employees [47]. Such monitoring allows for potential discriminatory practices by employers and health insurance companies.

Another source of sensitive information is the reviews that users leave when commenting and rating mobile applications on Google Play or iTunes, or even when purchasing from e-commerce websites. Some reviews may reveal information that falls under the "protected health information" category, including medical diagnoses and health conditions. The posts are not always anonymized, and once this information is available online, there is no control over sharing and reuse of such information by untrusted parties.

10.2.3 Process and Services

The main issue with data collection through mobile sensors is associated with excessive data collection, mainly due to organizations not knowing upfront what information is useful for them. Hence, they collect more data than the application needs, planning on future opportunities for data analysis and capitalization. Despite direct use by individual users, the collected data provides valuable information about their families, relatives, caregivers, and contacts. Such individuals, despite also being affected, are neither aware nor in agreement with data collection and potential analysis for further inferences. Depending on the sensors deployed for patient monitoring (e.g., camera, GPS, and microphone), personally identifiable information of others is also collected, indirectly impacting their privacy [7].

To prevent unauthorized access during transmission, trusted protocols with authentication and firewalls need to be used. Those ensure the delivery of records and data from authentic sources to legitimate parties. When data is published, e.g., for announcements, notifications, or reports, care must be taken to properly

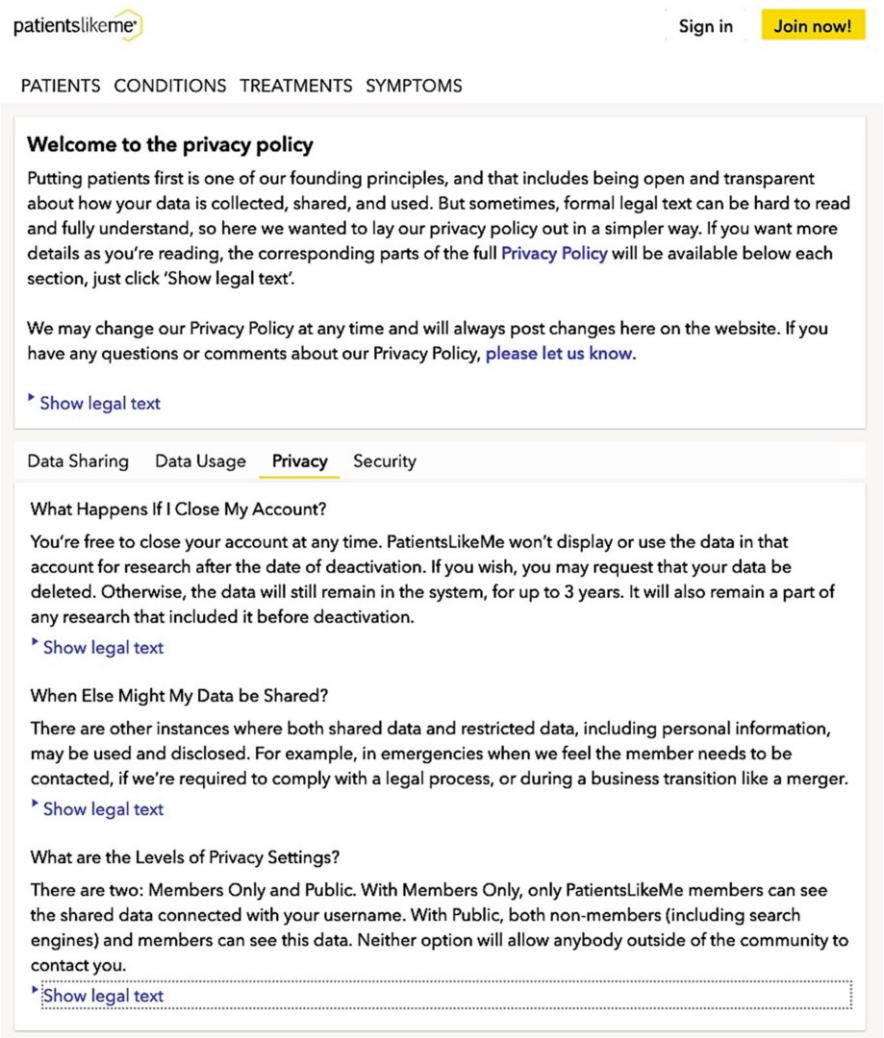

Fig. 10.2 Privacy policy of PatientsLikeMe including specifications of data sharing, usage, and security aspects (from https://www.patientslikeme.com/, as of November 4, 2019). The policy is copyright protected by PatientsLikeMe and used with permission

anonymize and de-identify it. In terms of access control, a combination of procedures is needed in order to (1) prevent non-authorized access to protected data, (2) avoid authentication issues, such as impersonation and spoofing attacks, and (3) ensure that users appropriately use the available privacy control mechanisms. In addition to controlling user access and privileges to prevent data access by unauthorized parties and tampering, the storage services should keep the patient's

records in an encrypted format. Data disposal should also be controlled, be it through shredding physical copies (notes, printed reports, exam results, etc.) or permanently deleting digital records.

10.2.4 Trade-Offs

While the confidentiality of medical records to preserve patients' privacy is undeniable, healthcare privacy involves important trade-offs regarding safety, security, automation, ease of use, efficiency, fairness, and individual versus collective benefits. Excessive protections pose serious obstacles to the provision of medical care [22]. While confidentiality is essential for preserving the relationship between doctors and patients, patient privacy and the associated privacy-preserving technologies should not be seen as a barrier to providing reliable healthcare to patients.

Privacy controls ensure that patients have the right to be informed about their conditions and treatments so that they can act accordingly. The information about privacy controls should neither overload nor overwhelm patients. In practice, clinical decision support systems should strive for efficiency while facilitating informed decisions from patients and practitioners. The communication and language should be adapted to the literacy level of individuals, and examples need to be provided.

Fully preventing all opportunities for data access is not ideal, since practitioners and researchers can obtain valuable insight from the collective and comparative analysis of data from a large cohort of patients. The knowledge gained with aggregated analysis involves the efficacy of treatments based on the patients' profiles, genetic information, and lifestyles, as well as the relations between the incidence of certain diseases, environmental data, and cultural aspects. Fully automating privacy choices, although feasible [23], is not ideal, as algorithms rely on generalizations that can lead to biased choices and discriminatory practices, besides also reinforcing inequalities [17].

A tension also exists between the safety and security priorities, as restricted access constrains the use of data that may be critical in emergency [24]. The knowledge generated from employing different treatments and assessing their respective health outcomes is relevant to inform and improve healthcare services. At the global scale, diagnostics can also inform epidemic trends, help in disease prevention, and inform healthcare policies. Benefits for public health and medical progress are well recognized [25]; for instance, when practitioners had to address the Zika outbreak in Latin America, the Ebola crisis in Africa, and the opioid crisis in the USA, the availability of information about the cases allowed practitioners to define a contingency plan, decide on health campaigns, and plan their responses. Hence, privacy policies must be carefully established to not hinder domain advancements and facilitate healthcare delivery. Still, there are risks around healthcare privacy, and the implications go beyond data breaches, shame, and embarrassment [16, 22]. Other disadvantages include increased insurance premiums, loss of benefits, and discriminatory practices. Potential for serious harm also involves loss of insurance, unemployability, and stigmatization [25].

Among the key benefits of data sharing, we highlight the opportunity to improve patient care with more informed decisions. Datasets that are not only larger but also more diverse can help inform and enhance current healthcare practices. The inference of data generated by a large number of patients and collected longitudinally contributes to medical research advancements. Using data from multiple sources can be particularly beneficial to support personalized healthcare and precision medicine. More specifically, patients benefit if their practitioners have access to information that can help them make better informed decisions, such as the patient's history and profile, information about previous procedures, ongoing treatments, genetic information, or even potential allergies that could put the patient at risk. The analysis of individual data from multiple sources can aid in diagnostic and therapeutic decisions, better suited to the patient's needs. While record keeping and sharing foster data analysis, the optimization of current processes requires efforts to prevent breaches and vulnerabilities. On the negative side, the exchange of information across multiple parties increases the likelihood of exploitation, as the data collected and not managed according to privacy principles may be used for the patient's disadvantage by health insurance companies, employers, third-party services, and others.

10.3 Regulations

Security and compliance drivers for privacy practices and controls include regulatory mechanisms, such as standards, laws, and frameworks. Regulatory mechanisms serve different levels of care—state, federal, or continent—and include European regulations, such as the GDPR [26], US-based laws, such as HIPAA [14], or Africa-specific regulations [16]. In the USA, those mechanisms include the Protected Health Information (PHI), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), and Food and Drug Administration (FDA). Such legislation is required to (1) ensure privacy, (2) improve patient care, and (3) enhance the usefulness and reliability of health information [22]. Also, their rules encourage a greater use of EHRs and other types of health information while protecting information privacy and security [27]. This section describes the main regulations addressing privacy in healthcare, including acts, legislation, rules, administrative agencies, safeguards, policies, procedures, forms, and toolkits.

10.3.1 Acts

Acts are descriptive pieces of legislation specifically applicable to circumstances and people. Acts are created in the parliament and need to be voted on by ministers before becoming laws. In the USA, three acts focus on privacy of health data,

HIPAA, HITECH, and Cures Act, whereas COPPA, FERPA, RFPA, and ADA handle tangential privacy information (education, disabilities, finances). They are defined as follows.

HIPAA The Health Insurance Portability and Accountability Act supports the sharing of health information among healthcare providers, health plans, and those operating on their behalf [28, 57]. HIPAA covers the treatment, payment, and other medical operations, besides providing channels for transmitting health information to relatives involved in the care of an individual as well as for research, public health, and other activities. Civil and criminal penalties apply when HIPAA regulations are not respected [14]. While HIPAA is a de facto standard regarding health regulation in the USA, updates are needed to ensure it also considers medical data extracted from health apps and the data collected by companies, e.g., searches for medical information [11].

HITECH The Health Information Technology for Economic and Clinical Health Act was signed in 2009 to promote the adoption and meaningful use of health information technology and EHRs [27, 41, 58]. Unlike HIPAA, HITECH is centered around digital records. Subtitle D of HITECH addresses the privacy and security concerns associated with electronic transmission of health information, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules [30] and apply violation penalties that range from US$100 to a US$1.5 million per year [29].

21st Century Cures Act (Cures Act) The Cures Act defines interoperability as the exchange and use of electronic health information, without burdening the user or blocking information access [31]. Additionally, this act facilitates the regulation of privacy controls in medical research, for instance, by waiving patients' consent when it is unnecessary and streamlining the approval processes for drugs and devices.

COPPA Enacted in 1998, COPPA limits the collection of personally identifiable information from youngsters without their parents' consent. The Commission's Rule implementing COPPA, effective since 2000, requires websites to post a complete privacy policy, notify parents about their information collection practices, and get verifiable parental consent before collecting personal information from their children or sharing it with others [32].

FERPA The Family Educational Rights and Privacy Act is a federal privacy law that gives parents protection concerning their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules [30].

RFPA The 1978 Right to Financial Privacy Act establishes specific procedures that federal government authorities must follow to obtain information from a financial institution about a customer's financial records [56].

ADA The Americans with Disabilities Act is a civil rights law forbidding discrimination acts against individuals with disabilities. ADA covers public life, jobs, schools, transportation, and all public and private places that are open to the public [39]. The law ensures that people with disabilities have the same rights and opportunities as everyone else [20]. As the technology evolves, updates were proposed to extend the protection, for instance, to prevent discrimination to deny job opportunities from individuals, whose predicted health outcomes include higher risks for disabilities [11, 40].

ACA The Affordable Care Act is a US federal status that covers health insurance plans for essential health benefits, including doctor's services, inpatient and outpatient care, prescription drug coverage, pregnancy and childbirth, and mental health services. These services are accessible for US citizens or lawful immigrants and aim at reducing healthcare costs, improving its quality, and expanding healthcare delivery to patients with a low income [33].

10.3.2 Legislation, Administrative Agencies, and Rules

Legislation consists of the enactment of the law owing to the provision of guidelines that dictate how the acts should be applied in practice. That is, legislation describes legal requirements and punishments for law violations. Legislation encompasses multiple acts. In the medical context, the Health IT Legislation includes the HITECH Act, the Cures Act, the Affordable Care Act, and the HIPAA. This legislation seeks to improve the exchange of electronic health information, by advancing interoperability, prohibiting information blocking, and enhancing the privacy of health technologies, so that multiple stakeholders, including patients, families, and healthcare practitioners, have access to electronic health information. To reinforce the legislation, regulatory agencies have been created. In the healthcare arena, the Food and Drug Administration (FDA) is a regulatory agency that enforces laws and protects public health, by ensuring the safety, efficacy, and security of drugs, biological products, and medical devices. The FDA also accepts requests for privacy acts.

While laws have legal consequences and actions associated with them, rules tend to be more flexible and carry milder consequences. Also, laws are sets of rules subject to legislative approval processes that have to be applied to everyone in a society. A rule is created by an executive branch, while a law is created by a legislative process. While the rules are enforced like laws, the laws carry a more formal connotation. In practice, both words are often used interchangeably. In the healthcare context, to regulate data and user privacy, four rules stand out.

The Privacy, Security, and Breach Notification Rules Implemented at the federal level under HIPAA, these are administered by the HHS Office for Civil Rights. Such rules establish a baseline of privacy protections and rights of patients and serve as the foundation of protections for individually identifiable health information and

of individuals' rights with respect to their information [34]. These rules require that entities notify all individuals affected by a breach, informing them when an unauthorized disclosure or use of their data occurs.

The Privacy Rule Also implemented under HIPAA, this is a standard for Privacy of Individually Identifiable Health Information aimed at assuring protection to the individuals' health information, without preventing the flow of health information needed to provide quality healthcare. This rule seeks to balance appropriate usage of information with privacy protection for individuals seeking medical care [19]. This rule is applicable to healthcare providers and health plans, who should implement administrative, technical, and physical safeguards to ensure privacy of health information.

The Security Rule Also implemented under HIPAA, the rule requires entities to evaluate risks and vulnerabilities in their environments and implement appropriate security measures to prevent threats and hazards to the integrity of protected health information [34]. This rule is a national standard in the USA, affecting all entities managing protected health information. The main difference between the privacy and the security rule is that the latter deals with protected electronic health information that is created, maintained, used, or received, whereas the former ensures individuals' rights to control their protected health information.

The General Data Protection Regulation (GDPR) Implemented in the European Union since 2018, GDPR focuses on individual rights and control in a digital economy. GDPR improved the levels of transparency and fairness, informing users about the use of their data and allowing additional control. Also, it enforces that medical information is only accessible for health and social care purposes, and to address public health concerns, after the patient or their legal guardian consent. If users want to know what data is available, they can request to access it and delete it if desired. By allowing users to delete their data, GDPR also enables users to be *forgotten* [26].

GDPR provides eight rights to individual users, which are defined in Table 10.1. Notably, GDPR follows the European model, which requires approval for any data collection and usage. This opt-in strategy prohibits the reuse of data for unintended purposes as well. While the opt-in choice is frequently bypassed with dubious practices that deceive users to select the wrong choice in an interface, the "don't reuse" clause ensures that selling user data is illegal [11].

It should be highlighted that the existing rules are complementary. They have been devised to address previous incidents, and they require technology support to be implemented in medical systems. More specifically, technologists should reinforce authentication mechanisms, keep track of the users' actions, allow data deletion, and deploy careful access controls.

Table 10.1 The eight individual rights of GDPR

The right to be informed: about data collected and used
The right of access: all the data collected upon request
The right to rectification: in case personal data is inaccurate or incomplete
The right to erasure: to delete all the personal information previously collected
The right to restrict processing: to refrain further usage of data already collected
The right to data portability: allows individuals to reuse their data, by moving, copying, or transferring it across IT environments
The right to object: to stop data being used for marketing or other purposes
The rights related to automated decision making and profiling: to prevent harm from automated decision making and allow users to request human intervention or challenge a decision

10.3.3 Safeguards, Policies, Procedures, and Forms

Safeguards, policies, procedures, and forms aim at protecting the patient's privacy with concrete actions and documents.

Administrative, Physical, and Technical Safeguards These are complementary approaches combining actions, procedures, measures, and policies for protecting medical data. Safeguards involve people, information, and facilities [13]. Physical safeguards protect buildings, equipment, and systems from unauthorized access. Administrative safeguards cover actions, policies, and procedures that regulate how practitioners protect information. Technical safeguards are system controls to prevent unauthorized access due to intrusion, tampering, or inappropriate deletion. To identify pertinent actions and procedures, a risk analysis is primarily executed. Once the risks are identified and analyzed, an action plan of security measures is developed and implemented.

Technical safeguards also include principles and procedures that should be followed, for instance, to ensure accountability and anonymization. Four common types of safeguards include:

Accountability This consists of logging all the operations executed by a system, so in case of breaches, the documentation enables investigation and audit. Accountability is enforced by administrative procedures and enabled through technical and physical solutions, including log-in systems and badges.

Anonymization and De-identification of Health Information This can be ensured when the data neither identifies nor provides sufficient information to identify an individual. To de-identify information, either a qualified statistician performs data analysis to detect the uniqueness of information, or individual identifiers are removed following established heuristics. In the former approach, either additional data is included or unique values for certain records or variables are modified. In the later approach, identifiers referring to the individual's relatives, household members, and employers are also removed [19].

Individual Choice This facilitates users taking more informed decisions by ensuring that reasonable information is provided about the data collection, usage, and dissemination. Also, individuals are given the option to either protect or reveal information. To inform individuals, a consent form is distributed.

Informed Consent Form This is a comprehensive document that informs users about the risks and benefits of a procedure. Written in an accessible language, this form lets users know that they can withdraw during a treatment and whom they need to contact with questions. Informed consent is a common practice in health services explaining the risks and benefits of a procedure. Although these forms lack flexibility for negotiation, they raise user awareness of data management and provide them options to act if needed.

To help with the technical implementation of privacy and security, the NIST HIPAA Security Toolkit Application was developed by the National Institute of Standards and Technology (NIST). This toolkit, provided by the Healthcare Information and Management Systems Society, covers concrete implementations of privacy and security, supporting organizations in understanding the requirements of HIPAA, implementing these requirements, and evaluating their implementations. Although the above procedures, policies, and protocols help regulating the implementation of privacy, additional efforts by public authorities and regulatory agencies are required to enforce enactment. Joint efforts from individuals, organizations, and government also need to be combined.

10.4 Limitations and Challenges in Current Practices

The state of practice and existing legislation around privacy-preserving controls in healthcare are limited in several aspects. The limited understanding of privacy risks and the lack of support tools to implement privacy controls result in reactive measures. As technology advances and novel privacy breaches are discovered, regulatory frameworks emerge. The problem with such regulations is that they are reactive and respond to past incidents. Proactive measures are rare and the attention paid to enact privacy and confidentiality in healthcare is still limited [22]. Thus far, in practice, most actions to address privacy issues have been limited and inconsistent, increasing vulnerability risks.

The fact that the existing solutions are fragmented and not unified leads to inconsistencies between legislation and practice. No comprehensive federal law protects the privacy of health records, while state laws are scattered and inconsistent [22]. Although HIPAA regulates protected medical data, it is by no means sufficient to exhaustively address problems that emerge with novel technologies. Several important conflicts of interest exist between the parties involved, including patients, healthcare practitioners, insurers, and third-party companies. The resulting trade-offs must be carefully resolved to ensure patients' privacy. For example, the use of social media channels for medical communications may result in disclosure with third-party organizations that can capitalize on the generated information even when users are oblivious of this [16].

Open questions remain concerning data ownership and governance. While end users generate large volumes of data, the ownership of such data is unclear when regulations are lacking and policies are ambiguous. The subjective interpretation of legal documents and lack of clear resolutions by companies may result in legal disputes. Despite collecting personal data, fitness trackers and smartwatches, for instance, are neither regulated by medical policies nor have FDA approvals in the USA. Although novel technologies collect physiological and activity data from users, the devices, applications, and services remain largely unregulated from a medical standpoint.

A higher privacy risk is faced by vulnerable populations, marginalized groups, and minorities, not only because their personal data can be used as a commodity, but also because privacy-preserving controls were not devised with their involvement. Although advances in privacy solutions have increased in the recent decades, most work has been concentrated on developed nations [35] and WEIRD (western, educated, industrialized, rich, and democratic) populations [36]. Also, there is a limited understanding of cross-cultural trust [37] and privacy [16] concerns, especially among users from underdeveloped countries and low socioeconomic status where eHealth regulation is nonexistent or fragmented. In addition, in some countries, e.g., Singapore, China, and Russia, online user data is heavily regulated and sometimes controlled by the government.

For the end users, be it a patient or legally responsible individual (caregiver or guardian), there is a trade-off between benefiting from technological resources and spending time and effort to understand and set privacy controls. While the access to paper-based records is limited due to spatial restrictions, EHRs increase the risks associated with data sharing and patient privacy, mainly due to the increased amount of information being collected and stored, and the larger number of parties remotely accessing this information. While in theory, most patients and caregivers prefer to have granular control over access to their data [38], enacting such control is time-consuming and burdensome, as it is not always feasible to analyze and select the best disclosure options [29].

In summary, the main limitations and challenges faced by the current practices are:

- **Existing solutions tend to be reactive** created in response to incidents because not all concerns are foreseeable and support tools are lacking.
- **Existing solutions are fragmented**, and the lack of a unified approach leads to inconsistencies in legislation, policies, and safeguards.
- **Conflicts of interest** hinder companies and organizations from matching privacy-preserving solutions with the best interest of users.
- **Gaps exist on data governance**, and open questions remain regarding data ownership.
- **Privacy controls are devised for an average user**, and vulnerable populations and marginalized groups face higher risks.
- **Users prefer fine-grained controls**, although it is time-consuming to navigate existing policies and configure access controls.

10.5 Recommendations

Given the numerous challenges involved in the implementation of privacy controls, a set of measures is necessary to ensure that effective controls are available.

Training and education efforts are necessary to prepare the workforce and raise user awareness. All the personnel involved in data collection and management, including patients and practitioners, need to be trained on privacy practices. By raising awareness of privacy concerns, they become better prepared to keep the systems up to date and protected. Practitioners should also check that the access control ensures a proper match between the datasets and the authorized personnel given specific privileges.

Enforcement of best practices and privacy measures ensures that access controls are properly deployed. Privacy-enhancing practices across stakeholders involve understanding the benefits one can have by sharing data. Incentives, rewards, as well as violation penalties, including settlements and fines, help ensure that stakeholders comply with standards and regulatory requirements.

As Fig. 10.3 illustrates, the recommendations to effectively implement solutions for privacy-enhancing technologies in healthcare involve multiple stakeholders and devices. Such solutions cut across data processing (request, analysis, retrieval) and storage services, be those physical (servers, hard drives) or virtual (running in the cloud).

In general, the recommendations proposed to implement privacy controls include training, monitoring, compliance, and accountability. Privacy-preserving principles and laws primarily consider the transparency of data handling, the control over data access, the accountability of user actions, and the interoperability to enable exchange of data across systems and organizations [31]. Specifically, transparency informs users about how their data is handled, facilitating trust in the systems. Control allows users to select what data they agree to collect and share and how the disclosure occurs. Accountability aims at logging and monitoring the usage of data and resources by users or systems, facilitating the analysis of executed operations.

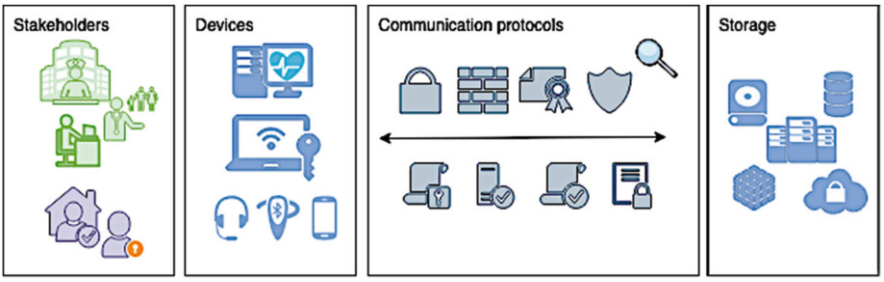

Fig. 10.3 Privacy-enhancing solutions include training various stakeholders, protecting the data storage and communication devices and infrastructure, strengthening the communication protocols, and protecting the devices and storage services

Interoperability facilitates the exchange of information, data aggregation, and analytics and also helps to ensure consistency in data sharing communication protocols.

To describe in detail the current practices and recommendations for privacy controls, the following subsections are structured per every stakeholder. The roles considered range from healthcare practitioners to third-party organizations.

10.5.1 Healthcare Practitioners

All the stakeholders involved in healthcare services generate health data and have access to patient's data from different sources, including lab results, medical imaging, and reports. When healthcare practitioners access medical records other than their own, the analysis of such external data helps to inform diagnostic and therapeutic decisions. Considering, for instance, rare diseases, it is beneficial for physicians to study health outcomes from other patients to better understand the patient's prognosis.

Practices and measures that can address privacy concerns include:

- **Educating and training workforce**. The personnel and staff managing patient data, medical equipment, and any technology involved in the data life cycle should be aware of potential risks, the legislation, and best privacy practices.
- **Certifying that personnel possess the skills needed to manage information appropriately**. The workforce should be qualified through training and evaluation sessions. Besides explaining the rationale and motivation for sharing patient data, healthcare practitioners should also clarify what data is shared, with whom, when, and for how long.
- **Performing a comprehensive risk analysis**. The analysis of risks should be conducted when a technology is introduced and also periodically to check whether upgrades or changes are needed. Such an analysis helps to detect the flaws and weaknesses of security and privacy in a healthcare facility or system and allows for defining and implementing an action plan to mitigate potential issues.
- **Conducting periodic verifications to ensure compliance with regulatory practices**. The training of the personnel and the risk analysis helps to ensure compliance. However, when relying on third-party services for data management, health providers must also ensure that these solutions are compliant with the necessary privacy requirements and regulations.
- **Selecting carefully all health providers**. Clinics, laboratories, external services, and vendors must be verified to ensure they are trusted parties that also adhere to legal requirements when handling medical data.

Some recommendations and best practices concern the communication between practitioners and patients (or legally responsible individual). In this context, healthcare practitioners including physicians should:

- **Advise patients and caregivers to adopt reliable communication channels**. For accountability and data protection, practitioners should remind patients to use trusted and secure communication channels, like tools and websites recommended by the organization for sharing sensitive information.
- **Inform patients about the choices they have regarding information sharing**. Practitioners should inform and remind their patients when they have choices concerning the disclosure of information with external parties, at different granularity levels, e.g., controlling under which circumstances laboratories and clinics may be allowed to share medical data to other organizations or stakeholders.
- **Ask patients' permission regarding the use of data and disclosing beyond the scope of the consultation**. Practitioners need to ask for patients' authorization to use their data in unconventional ways, for instance for the purpose of scientific investigation or advertisement from merchants.
- **Inform patients about consent forms and data sharing procedures**. Practitioners should allow patients or caregivers, guardians, and legal representatives to provide informed consent and authorization for data sharing when necessary.
- **Adopt accessible language and mindful approach to seek consent**. Healthcare professionals should provide patients with information related to the benefits of sharing data in a transparent and neutral way and use clear and appropriate language and tone [25].

The benefits associated with data sharing go beyond individual's advantages in the short run to collective advantages in the long run. Transparency when dealing with sharing practices of health services is essential to build trust between agencies and users and enable legitimate informed consent. Therefore, all the risks and benefits should be properly disclosed.

10.5.2 Patients and Caregivers

The benefits for patients and caregivers when sharing protected information include the knowledge gained from the exchange of information and advice received from building a network of social support. In contrast, the major drawback of sharing information is a potential loss of control over data dissemination and opportunities for misuse.

Other benefits from data sharing are large information repositories built from the aggregated data, allowing for a stronger support for evidence-based medicine, which not only advances the current knowledge on healthcare delivery but also enhances the potential for preventive and precision medicine. Preventive medicine focuses on adopting measures that either avoid the occurrence of a condition or prevent the exacerbation of symptoms when a condition has already been diagnosed.

Precision (or personalized) medicine aims at tailoring individual treatments, medical decisions, and products to the patient profile in a unique and patient-centric way.

For patients and caregivers, measures that help to protect their privacy include:

- **Installing software updates** to keep the systems in use upgraded and prevent potential attacks and vulnerabilities.
- **Using strong authentication mechanisms** by choosing strong passwords as well as two-factor authentication to log in.
- **Employing reliable communication channels**. End users should rely only on trusted channels when communicating medical information. Preference should be given to secured networks and authenticated personal devices.
- **Refraining from posting sensitive information** in online forums, public websites, social media channels, discussion boards, and online communities.
- **Assessing impacts and risks**. Patients and caregivers should note that disclosing sensitive medical data, e.g., hereditary conditions, affects not only the patient but also their relatives. To prevent mistakes, users should be aware of major privacy risks and learn the ways to prevent issues or recover from them.
- **Taking informed decisions**. Control mechanisms should ensure that patients or their guardians and caregivers are aware of the risks and benefits of data collection, monitoring, and sharing [25, 29] to select sharing preferences. If that is not the case, patients and caregivers should seek for additional clarifications.

Although training is helpful, one cannot expect end users to be privacy experts. Therefore, privacy control mechanisms should be implemented for and with end users, striving for ease of use, high usability, efficiency, and sustained adherence. Simple measures, like relying on trusted communication channels to exchange information, can help reduce the risk of unintended access. When available, privacy controls should be intuitive and transparent, proactively informing end users, and allowing them to opt in or out of data sharing according to their individual preferences. Privacy choices must allow granular controls and inform users in accessible language.

10.5.3 Insurance Companies

Electronic health records (EHRs) are medical records storing information about consultations, allergies, diagnosis, and the medical history of a patient. EHRs handled by insurance companies contain information about the financial transactions related to treatments, medical procedures, and the list of practitioners in the patient's network. To ensure privacy, the network of health providers of the insurer should encompass trusted parties, including not only practitioners, but also clinics offering examination or therapeutical services, as well as vendors of medical equipment and assistive technologies.

Another recommendation includes informing the patients about current practices around management of their health data. Terms and conditions must be made

available to end users for verification. Systems from insurers should also provide interfaces for privacy controls that are easy to use, adopt, and sustain engagement. Design decisions for user interfaces and interaction must follow standard usability practices, ensuring that the settings are accessible for patients and caregivers and adequate to meet their specific health and digital literacy skills [29].

Lastly, insurance systems managing health records should give users enough flexibility for negotiation and decision making about the ways their data is shared. Flexibility includes giving users the ability to revoke or control data access by setting who has access to the data, when, and under what circumstances and conditions. In summary, the recommendations for insurance companies include:

- **Selecting trusted parties to work with**, ensuring that services in the network are reliable and comply with privacy policies
- **Ensuring compliance with existing healthcare privacy policies**, by following their guidelines and standards, conducting risk analysis and periodic assessments, providing training to personnel, and conducting compliance checks
- **Informing patients, caregivers, and legal responsible** about current privacy practices, describing in an accessible language what practices are employed to secure patients' data and not disclose it
- **Giving users control over data sharing** practices by allowing patients to select who has access to their data and under what conditions

10.5.4 Technologists

Privacy must be prioritized in the implementation of healthcare infrastructures. Rather than an add-on patchwork, privacy concerns should be thoroughly considered since the beginning of the design and development phases to ensure confidentiality, integrity, and availability of medical data. Existing systems implemented without privacy controls should be updated accordingly, to comply with recent privacy standards and policies.

To ensure privacy is preserved, a holistic approach should be adopted. Technologists need to consider the datasets in use, the entire ecosystem of devices, and the underlying systems and networks. At the data level, measures such as de-identification and anonymization have proven insufficient to guarantee that personally identifiable information is not disclosed [9]. A notorious case is the public release of the search history of 20 million search queries collected by AOL. Although the names of the users were not disclosed, the content of the queries was sufficient to trace the users' identities back. While the intention of publicly releasing the data was to support research, it ended up revealing private information, including health-related topics that users did not authorize [29]. Thus, more comprehensive and up-to-date solutions are required. Differential privacy, nudging privacy, and contextual privacy are some of the frameworks that should be adopted to facilitate the implementation of privacy-preserving technologies.

Overall, for data collection, only data essential to the analysis should be extracted, to minimize unintended disclosure risk. However, there are many benefits of scientific investigations exploring the potential of data for knowledge discovery. In these cases, patients should be informed about the data collected and given the choice to decide how it is used for scientific discoveries. In terms of implementation, a modularized architecture helps to prevent unintended access, by ensuring that certain modules of the program and application are only accessible to users with certain privileges in the system. The patient profile, for instance, could be implemented as a module, isolated from consultation schedule, medical history, etc. Regarding storage, the data should be encrypted to prevent unauthorized access and tampering. Access control mechanisms should be implemented to protect assets from unauthorized access.

At the physical level, the networks should be protected with firewalls, and the authentication mechanisms should be secured to ensure proper access control, for instance reinforcing two-factor authentication. Medical devices, such as pacemakers and defibrillators, should be subject to risk analysis and made secure to prevent attacks [24]. At the system level, access control mechanisms should ensure that only authorized personnel can access medical data upon authentication, employing highly controlled environments to avoid vulnerabilities. Also, the activity of the users should be logged, enabling auditing procedures in case a breach occurs.

Concluding the recommendations for technologists, the following are highlighted:

- **Prioritizing privacy in the design and development process** to cover it in the network, architectural, and database design and implementation in a holistic manner that spans across devices and systems
- **Adopting a modularized system architecture** to prevent access to services, resources, and data across parts of the application
- **Implementing encryption in data transfer or storage** to ensure that in case of unauthorized access during transmission, the content is not disclosed to external parties
- **Verifying the compliance of the systems** with current norms, to check whether the technology preserves data and users' privacy according to the standards and policies in practice
- **Adopting up-to-date privacy practices** to facilitate user control and ensure that the disclosed data is anonymized and de-identified as necessary

10.5.5 Regulators

In crafting the legislation, perspectives of technologists, domain experts, and legislators need to be triangulated, combining a bottom-up approach considering the needs of citizens and patients with a top-down one considering the government resources and obligations. For policy makers and regulators to decide what must

be implemented in a healthcare facility to assure privacy of medical records and patients, they have to also consult with domain experts and technologists, to better understand the context in which a health service is delivered, and the capabilities and limitations of the digital realm. Altogether with legal consultants, domain experts and technologists can inform regulators on the governmental and legislation requirements for medical data.

Technologists will be aware of the potential vulnerabilities and breaches, knowing the strengths and weaknesses of the technology, and best practices to prevent problems and recover from them. Domain experts understand what data types are at stake and are familiar with the needs of patients and caregivers. Such knowledge combined helps to inform regulators in making decisions about privacy in healthcare. The technologists also need to notify regulators promptly, so that the regulators are kept up to date and they can update the legislation accordingly, when novel risks emerge, or vulnerabilities and breaches are discovered.

To facilitate this effort, the US Department of Health and Human Services' Office for Civil Rights started publishing healthcare data breach reports. By sharing what organizations were compromised, how they were affected, and the financial impacts of the attacks, the public reporting of breaches helps users to understand how their data is compromised so they take appropriate actions to prevent future problems. Additionally, it helps them to choose more trustworthy organizations. While still offering a reactive solution, breach reports inform technologists on potential issues, so that they can work on preventing, mitigating, and addressing such problems in more efficient ways by defining best implementation practices, standards, and guidelines.

Besides creating policies and guidelines, another responsibility of such stakeholders is enforcing that privacy requirements are properly addressed, to ensure that policies created for data protection and privacy are enacted. This effort should not only incentivize organizations to adopt privacy-preserving solutions but also punish organizations not compliant with current norms, standards, and policies.

In summary, the recommendations for regulators are defined as follows:

- **Communicate early with domain experts and technologists**, since their perspectives are essential to decide on the legislation and since combining a bottom-up with a top-down approach helps to holistically address privacy.
- **Enforce legislation** using proactive incentives and reactive penalties to punish organizations not conforming to existing regulations.
- **Maintain up-to-date policies** to cover emerging technologies before incidents occur, consulting with technologists.
- **Facilitate the implementation of regulations** by informing organizations, using accessible language, and making training and education available.

10.5.6 Third-Party Organizations

Third-party organizations include commercial services that may take advantage of medical data using analyses and inference for advertisement and marketing purposes. It can also include banks, e-commerce applications, or even academic institutions conducting scientific investigation. Such service providers might benefit from patient's medical data and infer medical information about patients. Such information should be protected from unintended disclosure and regulated by respective policies.

Although HIPAA protects users' data from exploitation, clinics and organizations may set up agreements with service providers. In cases when third-party services are requested, users should be informed and have the choice to not disclose information. Even though external service providers oftentimes take advantage of the data collected, in addition to complying to current regulations, third-party services must ideally:

- **Be clear and transparent** with end users about the usage of their data.
- **Maintain secure practices to manage medical information**, by informing users in advance on the use of their personal data, and obtain informed consent to authorize the use of the data.
- **Provide users with flexibility to decide on the usage of their data**, including opt-in and opt-out choices as well as the ability to withdraw the authorization for sharing at any point in time, revoking data access.

10.6 Conclusion

This chapter provides an overview of privacy in the healthcare domain, listing the dimensions that should be considered when implementing privacy-preserving controls in this domain. To address the many risks involved with handling medical data in a digital infrastructure, a holistic approach is needed, cutting across implementation phases, multiple stakeholders, and assets. Privacy-enhancing solutions need to consider the dimensions in which privacy breaches may occur, from the data collection, through processing, storage, analysis, and sharing. In addition to considering the data life cycle, such dimensions also include multiple stakeholders, equipment, artifacts, and assets, guiding not only patients and caregivers as end users, but also healthcare practitioners, providers, insurance companies, laboratories, and clinics.

Despite the undeniable importance of privacy controls when managing health data, the implementation of these dimensions is complex, several questions remain open, and numerous considerations should be taken into account to ensure that patients' data is preserved and privacy controls effectively provide them the necessary levels of transparency, control, and trust. Future research and development

in the domain should ensure that patient privacy improves health outcomes and advances healthcare for patients and communities, rather than seen as a barrier impeding public health.

References

1. Lazar, A., and E.E. Dixon. 2019. Safe enough to share: Setting the dementia agenda online. *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–23.
2. Lorenzen-Huber, L., M. Boutain, L.J. Camp, K. Shankar, and K.H. Connelly. 2011. Privacy, technology, and aging: A proposed framework. *Ageing International* 36 (2): 232–252.
3. Motti, V.G. 2019, October. Designing emerging technologies for and with neurodiverse users. In *Proceedings of the 37th ACM International Conference on the Design of Communication,* 1–10.
4. Choi, Y.K., A. Lazar, G. Demiris, and H.J. Thompson. 2019. Emerging smart home technologies to facilitate engaging with aging. *Journal of Gerontological Nursing* 45 (12): 41–48.
5. Pradhan, A., A. Lazar, and L. Findlater. 2020. Use of intelligent voice assistants by older adults with low technology use. *ACM Transactions on Computer-Human Interaction (TOCHI)* 27 (4): 1–27.
6. Takemoto, M., T.M. Manini, D.E. Rosenberg, A. Lazar, Z.Z. Zlatar, S.K. Das, and J. Kerr. 2018. Diet and activity assessments and interventions using technology in older adults. *American Journal of Preventive Medicine* 55 (4): e105–e115.
7. Motti, V.G., and K. Caine. 2015. Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*, 231–244. Springer.
8. Lu, X., T.L. Reynolds, E. Jo, H. Hong, X. Page, Y. Chen, and D.A. Epstein. 2021. Comparing perspectives around human and technology support for contact tracing. In *CHI Conference on Human Factors in Computing Systems (CHI '21), Yokohama, Japan*, May 8–13, 2021. New York, NY: ACM.
9. Carrotte, E.R., I. Prichard, and M.S.C. Lim. 2017. "Fitspiration" on social media: A content analysis of gendered images. *Journal of Medical Internet Research* 19 (3): e95.
10. Abdullah, S., and T. Choudhury. 2018. Sensing technologies for monitoring serious mental illnesses. *IEEE MultiMedia* 25 (1): 61–75.
11. O'neil, C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.
12. Hill, K. 2012. How target figured out a teen girl was pregnant before her father did. *Forbes*. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#53c93a8e6668
13. Shapiro, D. 2019. How a DNA testing kit revealed a family secret hidden for 54 years. *Time*. time.com/5492642/dna-test-results-family-secret-biological-father/
14. U.S. Government Printing Office. 1996. *Insurance Portability and Accountability Act of 1996*. 104th US Congress, Washington, D.C. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/
15. De Choudhury, M., and S. De. 2014, May. Mental health discourse on reddit: Self-disclosure, social support, and anonymity. In *Eighth International AAAI Conference on Weblogs and Social Media*.
16. Namara, M., D. Wilkinson, B.M. Lowens, B.P. Knijnenburg, R. Orji, and R.L. Sekou. 2018, December. Cross-cultural perspectives on eHealth privacy in Africa. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, 7. ACM.
17. Marabelli, M., S. Newell, and X. Page. 2018. *Algorithmic Decision-Making in the US Healthcare Industry*. Presented at IFIP, 8.

18. Motti, V.G., and N. Kalantari. 2019. Understanding how social media imagery empowers caregivers: An analysis of microcephaly in Latin America. In *The 13th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth'19), Trento, Italy*, May 20–23, 2019. ACM.
19. Centers for Disease Control and Prevention. 2003. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. *MMWR: Morbidity and Mortality Weekly Report* 52 (1): 1–17.
20. Almulhem, A. 2012. Threat modeling for electronic health record systems. *Journal of Medical Systems* 36 (5): 2921–2926.
21. Brodey, D. 2019. Disability advocates poke holes in White House Plan to snoop on Facebook pages for disability fraud. *Forbes*. https://www.forbes.com/sites/denisebrodey/2019/03/11/disability-advocates-poke-holes-in-white-house-plan-to-snoop-on-facebook-pages-for-disability-fraud/
22. Goldman, J. 1998. Protecting privacy to improve health care: As the deadline for passing health privacy legislation in Congress nears, consensus is needed on a framework that values both patients' privacy and public health goals. *Health Affairs* 17 (6): 47–60.
23. Watson, J., H.R. Lipford, and A. Besmer. 2015. Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)* 22 (6): 32.
24. Halperin, D., T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, ... & W.H. Maisel. 2008, May. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy*, 129–142. IEEE.
25. Caine, K., S. Kohn, C. Lawrence, R. Hanania, E.M. Meslin, and W.M. Tierney. 2015. Designing a patient-centered user interface for access decisions about EHR data: Implications from patient interviews. *Journal of General Internal Medicine* 30 (1): 7–16.
26. Voigt, P., and A. Von dem Bussche. 2017. *The EU General Data Protection Regulation (GDPR). A Practical Guide*. 1st ed. Cham: Springer International.
27. Goldstein, M.M., and H.T. Jane. 2010. The first anniversary of the Health Information Technology for Economic and Clinical Health (HITECH) Act: The regulatory outlook for implementation. *Perspectives in Health Information Management/AHIMA* 7 (Summer).
28. Scaraglino, P. 2002. Complying with HIPAA: A guide for the university and its counsel. *JC & UL* 29: 525.
29. Barbaro, M., and T. Zeller. 2006. *A Face is Exposed for AOL Searcher No. 4417749*. https://www.nytimes.com/2006/08/09/technology/09aol.html
30. US Department of Education. 1974. Family educational rights and privacy act (FERPA).
31. Hudson, K.L., and F.S. Collins. 2017. The 21st Century Cures Act—a view from the NIH. *New England Journal of Medicine* 376 (2): 111–113.
32. Federal Trade Commission, and Federal Trade Commission. 2016. Children's online privacy protection rule ("COPPA").
33. Blumenthal, D., M. Abrams, & R. Nuzum. 2015. The affordable care act at 5 years.
34. Office for Civil Rights. 2017. *The HIPAA Security Rule*. https://www.hhs.gov/hipaa/for-professionals/security/index.html
35. Sambasivan, N., G. Checkley, A. Batool, N. Ahmed, D. Nemer, L.S. Gaytán-Lugo, ... E. Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS* 2018*)*, 127–142.
36. Henrich, J., S.J. Heine, and A. Norenzayan. 2010. The weirdest people in the world? *Behavioral and Brain Sciences* 33 (2-3): 61–83.
37. Berkovsky, S., R. Taib, Y. Hijikata, P. Braslavsky, and B. Knijnenburg. 2018. A cross-cultural analysis of trust in recommender systems. In *Proceedings of the* 26*th Conference on User Modeling, Adaptation and Personalization,* 285–289.
38. Bol, N., and J. Romano Bergstrom. 2015. Designing for vulnerable users: Illustrations (may) help understand complex health websites. *User Experience* 15.
39. Americans With Disabilities Act. 1991. Public Law 101–336. *Federal Register* 56 (144): 35,545–35,555.

40. Auxier, B.E., C.L. Buntain, P. Jaeger, J. Golbeck, and H. Kacorri. 2019, April. # HandsOffMyADA: A Twitter response to the ADA Education and Reform Act. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 527. ACM.
41. Blumenthal, D. 2010. Launching HITECH. *New England Journal of Medicine* 362 (5): 382–385.
42. De Choudhury, M., M. Gamon, S. Counts, and E. Horvitz. 2013, June. Predicting depression via social media. In *Seventh International AAAI Conference on Weblogs and Social Media*.
43. Greene, E., P. Proctor, and D. Kotz. 2018. Secure sharing of mHealth data streams through cryptographically-enforced access control. *Smart Health*.
44. Grundy, Q., K. Chiu, F. Held, A. Continella, L. Bero, and R. Holz. 2019. Data sharing practices of medicines related apps and the mobile ecosystem: Traffic, content, and network analysis. *BMJ* 364: l920.
45. Limbago, A.L. 2019. *Combating Digital Authoritarianism: U.S. Alternative Needed to Counter Data Localization and Government Control*. The National Security Institute. Technical Report.
46. Lowens, B., V.G. Motti, and K. Caine. 2017, August. Wearable privacy: Skeletons in the data closet. In *2017 IEEE International Conference on Healthcare Informatics (ICHI)*, 295–304. IEEE.
47. Mahdawi, A. 2019. There's a dark side to women's health apps: Menstrual surveillance. *The Guardian*.
48. McHugh, B.C., P. Wisniewski, M.B. Rosson, and J.M. Carroll. 2018. When social media traumatizes teens: The roles of online risk exposure, coping, and post-traumatic stress. *Internet Research* 28 (5): 1169–1188.
49. Melton, L. Joseph. 2000. Medical privacy. *Issues in Science and Technology* 17 (1): 12–13.
50. Motti, V.G., and K. Caine. 2015, September. An overview of wearable applications for healthcare: Requirements and challenges. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, 635–641. ACM.
51. Nurgalieva, L., A. Frik, F. Ceschel, S. Egelman, and M. Marchese. 2019. Information design in an aged care context: Views of older adults on information sharing in a care triad. In *The 13th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth'19), Trento, Italy*, May 20–23, 2019. New York, NY: ACM.
52. Office for Civil Rights. 2013. *The HIPAA Breach Notification Rule*.
53. O'Herrin, J.K., N. Fost, and K.A. Kudsk. 2004. Health Insurance Portability Accountability Act (HIPAA) regulations: Effect on medical record research. *Annals of Surgery* 239 (6): 772.
54. Reece, A.G., A.J. Reagan, K.L. Lix, P.S. Dodds, C.M. Danforth, and E.J. Langer. 2017. Forecasting the onset and course of mental illness with Twitter data. *Scientific Reports* 7 (1): 13006.
55. Serrano, K.J., M. Yu, W.T. Riley, V. Patel, P. Hughes, K. Marchesini, and A.A. Atienza. 2016. Willingness to exchange health information via mobile devices: Findings from a population-based survey. *The Annals of Family Medicine* 14 (1): 34–40.
56. Trubow, G.B., and D.L. Hudson. 1978. The Right to Financial Privacy Act of 1978: New protection from federal intrusion. *The John Marshall Journal of Practice and Procedure* 12: 487.
57. Department of Health and Human Services – The Office of the National Coordinator for Health Information Technology. *Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity*.
58. U.S. Department of Health and Human Services. *HITECH Programs*. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1487&parentname=CommunityPage&parentid=28&mode=2&in_hi_userid=11113
59. Zhang, S. 2019. The fertility Doctor's secret. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2019/04/fertility-doctor-donald-cline-secret-children/583249/