MEDICAL TECHNOLOGY: Establishing Patient and Consumer Trust

Medical devices have become increasingly complex, incorporating various sensors, software, and connectivity features to improve health outcomes. These technologies have significantly improved patient care by enabling real-time monitoring and data collection, personalized treatment plans, and remote access to healthcare services. Patients enjoy an elevated care experience that is less intrusive to their daily lives. Medical technology organizations receive a steady supply of data, ripe with opportunities to continue to improve care outcomes and innovation.

However, as medical devices have become more connected, they have also become more vulnerable to cyberattacks, data breaches, and privacy violations. Protected health information is particularly sensitive data that has the potential to seriously harm patients and consumers if breached or monetized in ways that are inconsistent with patient care and informed consent.

The risks associated with the improper handling of personal data are wide-ranging, forcing organizations to carefully assess and balance risk with the desired benefit. Medical technology organizations operate under complicated, multifaceted relationships with data, making it challenging to define who is responsible for data privacy. Organizations that interact with protected health information must integrate new privacy and data protection requirements within their existing efforts to comply with industry, state, national, and international standards and legislation.

NEW TECHNOLOGIES

Without the creation of new and inventive technologies to support healthcare, the rapid advancement of patient care would not be conceivable. The development of digital health solutions has been aided by advances in processing power, declining storage costs, improved connectivity, and advances in data analytics and artificial intelligence.

Mobile Medical Applications

Developers have taken advantage of mobile platform features to turn apps into medical devices or extensions of them. These apps provide clinicians with the ability to remotely collect and access patient data at any time, including physical activity levels, glucose levels, heart rate, and medical images. However, this enhanced flow of data to clinicians can come at a cost: not all products meet privacy and security standards, potentially giving rise to statutory and civil liability for privacy breaches, insecure data storage, and failure to obtain patient consent.[1]

Internet of Medical Things (IoMT)

The IoMT reflects the convergence of increased connectivity and advances in medical technology. This connected infrastructure of health systems boosts the speed and accuracy of diagnosis and treatment and provides the ability to monitor patient health in real-time. As the amount of sensitive data handled by the IoMT grows, so do the privacy and security concerns. These concerns go beyond mere compliance, as threats to the confidentiality, integrity, and availability of protected health information not only impact privacy rights but may also impact patient health if compromised.[2]

Artificial Intelligence (AI)

By drawing conclusions from the significant amount of data produced by medical devices, AI and machine learning technologies have the potential to expedite research, development, diagnosis, and treatment. These technologies are being used to find patterns in genetic data, photos, and medical records, and they are even being used to estimate the probability of life threatening health emergencies.[3] The use of AI, however, raises several new legal and ethical issues, such as how to control an algorithm and how to be open with data subjects when the "black box" of machine learning hides the reasons behind, methods of, and effects of, the decisions. While these "black box" artificial intelligence systems may not provide explanations on how the outcomes were reached, trained professionals can utilize a variety of methods to oversee the training and usage of AI. In conjunction with healthcare professionals, technologists can assist in cross-checking the decisions made by these AI models in both clinical and non-clinical contexts.

DATA ACCOUNTABILITY

Due to the complexity of data engagement in the medical technology space, it can be challenging to maintain regulatory compliance. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) compliance requirements were already challenging due to their expansive nature and lack of clear standards to achieve compliance. Now, medical technology organizations must manage and protect additional data, consider new regulations, and deal with regulatory enforcement bodies with enhanced penalties. In the increasingly cyber-dependent landscape, these enforcement actions are now coming from previously unrelated regulatory agencies such as the Federal Trade Commission (FTC). For example, a healthcare company specializing in telemedicine and discount prescriptions was recently fined $1.5 million by the FTC for sharing and monetizing private health data with third-party advertisers. This action relied on a previously unused 14-year-old health breach notification rule that is now becoming increasingly relevant.[4]

Under the current landscape of remote and connected technologies, data may be:

- collected directly from patients;
- transferred to a healthcare provider from patients or other healthcare providers;
- sent onward to medical technology organizations in identifiable or pseudonymous form;
- made available to third-party service providers to facilitate care;
- analyzed to improve performance; and
- potentially used in other ways that may or may not impact the patient or consumer.

With such a variety of complex circumstances for data collection, transfer, and use, even well-meaning organizations can have difficulty with the most basic question of protected health information privacy and governance: who is responsible for protecting this data?

To answer this question, organizations must understand the regulations surrounding this data; how tools are collecting, using, and transferring the data; the accountability requirements under applicable regulations; and the legal obligations associated with data collection, transfer, and use.

Further, pseudonymous data, under most privacy regulations, is not considered to be different than identifiable protected health information, and never having received identifiable data sets does not absolve an organization from data protection accountability. Until the data is eventually destroyed in line with retention laws, each organization will need to preserve its data, regulate access to it, oversee its usage in accordance with the agreed-upon processing activities, and prepare for and respond to breaches or events. Organizations must demonstrate that they are storing, managing, and protecting their data appropriately.

Designing for the User Experience

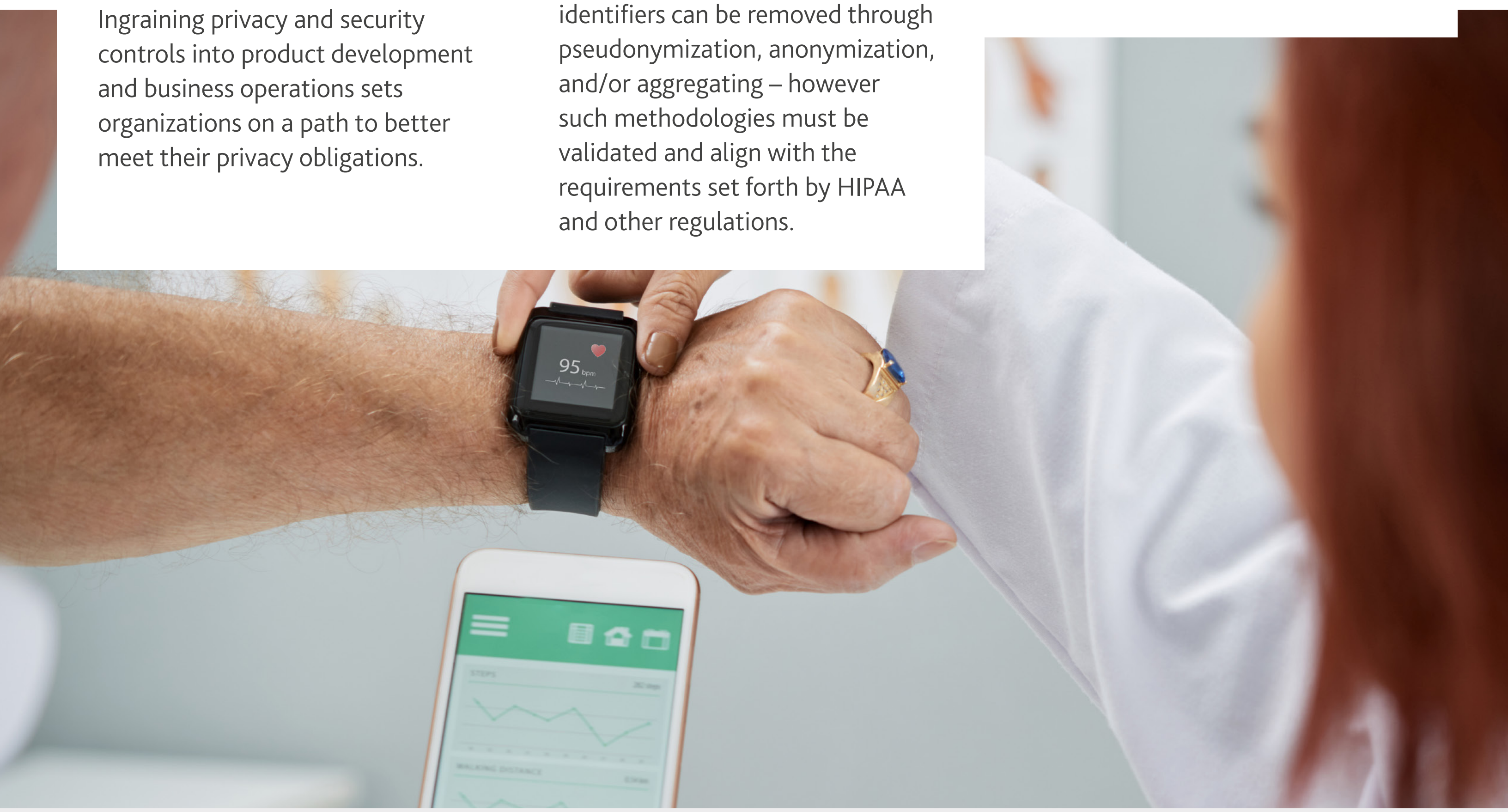
Access to large quantities of high-quality data is necessary for advancing medicine and patient care. However, the societal benefits of efficient and effective health solutions must be balanced with an individual's right to privacy. Some privacy laws and regulations, such as the European Union General Data Protection Regulation (GDPR), require organizations to apply Data Protection by Design and Default principles to their data handling practices. For medical technology organizations, this means that products and applications must be designed and developed to protect privacy as the default. Ingraining privacy and security controls into product development and business operations sets organizations on a path to better meet their privacy obligations.

Meeting User Expectations

Health data is now readily available because of new technology and data-sharing procedures. However, using it for purposes other than those for which it was first obtained presents ethical and legal problems. Before using patient or consumer data for reasons other than those explicitly outlined by HIPAA, including direct patient care, public health, or scientific study, organizations must typically obtain informed consent from the patient or customer. Although it is challenging to foresee all potential applications for data in the future, each use must be in line with the patient's consent. Before data is utilized for secondary purposes, identifiers can be removed through pseudonymization, anonymization, and/or aggregating – however such methodologies must be validated and align with the requirements set forth by HIPAA and other regulations.

Maintaining Trust in a Digital Age

The fast-moving digital landscape has not only challenged current privacy laws and regulations but also resulted in an erosion of public trust in how data is used and protected. Reports of misuse, nefarious monetization, and breach of data can also threaten an organization's reputation. As organizations adopt new strategies and products, they need to be proactive and transparent about their data policies and practices to make consumers comfortable with sharing their data. Transparency also helps consumers and regulators understand the benefits that data access brings to the medical field.



PRIVACY AND DATA PROTECTION

Privacy and Data Protection regulations have had a significant impact on medical devices, particularly those that process or transmit patient data. Medical technology manufacturers must build devices that are designed and developed in compliance with these regulations, which includes implementing appropriate technical and organizational measures to protect patient data, conducting regular security assessments, and possibly appointing (or outsourcing) a Data Protection Officer. Systems must be designed, and data flows must be compatible, with regulatory requirements for data access, rectification, and erasure. This may involve implementing additional software or hardware features to enable patients to access and manage their data.

Medical technology companies must also have systems in place to detect and respond to data breaches in a timely manner. These systems are critical to compliance with breach notification requirements. Failure to properly implement such systems can result in fines and reputational damage, as well as potential legal action from affected individuals. Even when such mechanisms are in place, the cost of notification alone can be significant. For example, the defendant in one such class action settlement spent millions to provide initial notifications to the public and affected individuals. This was largely due to the cost of postage and mailing of physical notifications highlighting the importance of proper privacy and data protection mechanisms.

BALANCING OPPORTUNITY WITH RISK

Medical technology organizations must balance the opportunity to provide innovative technical healthcare solutions with the real threat posed by collecting, processing, and transmitting protected health information. When developing business strategies, leaders in these organizations must understand privacy and data protection requirements as they assess the value and opportunity associated with the data they collect and use. Medical technology companies must develop and maintain proactive and thoughtful data protection regimes that not only address existing data regulations, but also consider future state, national, and international legislation.

People who know Life Sciences, know BDO.

www.bdo.com/**life-sciences**

For more information on how to implement data privacy and governance best practices at your organization, see our **Data Privacy and Governance Checklist**.

[1] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5008929/
[2] https://doi.org/10.1155/2018/5978636
[3] https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device
[4] https://news.bloomberglaw.com/privacy-and-data-security/goodrx-ftc-privacy-fine-is-warning-shot-for-health-tech-firms

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.