JUNE 2021
www.bdo.com/lifesciences

DATA PRIVACY AND DATA GOVERNANCE FOR LIFE SCIENCES

INSIGHTS FROM THE BDO LIFE SCIENCES PRACTICE

BDO

Interacting with personal information in the age of regulated data privacy is a gamut of risk, with most organizations carefully weighing the risk they're willing to shoulder against the business value they seek.

Some organizations, however, like those in the life sciences industry, are not afforded that luxury. Where other organizations choose when and where to engage with personal information, life sciences organizations are often forced to do so as a fundamental component of developing and providing their therapeutics, products or services. Where other organizations can easily determine responsibilities for managing data privacy, life sciences organizations often operate under complex, multi-faceted relationships with data. And where most organizations are just now developing an understanding of their privacy requirements, organizations that interact with protected health information (PHI) must integrate new regulatory requirements with efforts to comply with existing industry, state, national and international standards and legislation.

DECENTRALIZED STRATEGY FOR CARE

Compliance with PHI management laws that include data privacy requirements may not be new to all life sciences organizations, but the accompanying use cases can be both myriad and novel. Facilitated by a drastic rise in data collection, transfer and analytics capabilities, life sciences and healthcare operations that were once highly centralized are now increasingly remote. In-person care and services are now supplemented, or in some cases replaced, by telehealth offerings that support easier access to care for patients and consumers, reduce costs and improve the care experience.[1] Telehealth capabilities are now being applied to support decentralized clinical trials, which first saw a rise during the COVID-19 pandemic but are likely here to stay as a result of increased patient participation and retention.[2] Even the medical devices used to gather and monitor PHI have seen a fundamental evolution in recent years and are now themselves remote, wearable by the patient or consumer and backed by the connectivity needed to collect, store and transfer the resulting PHI. These wearable devices offer benefits to both the wearer and the life sciences organizations that utilize the data: consumers get a more passive care experience that is less intrusive to their daily lives, and care providers receive a constant flow of data instead of periodic samplings of results.[3]

But with this increased flow of data, less intrusive care experience and reduced costs (i.e., the value side of this data), comes risk. This ongoing delocalization of care provision, along with the benefits, drives an increase in the generation and processing of PHI. Simply put: life sciences organizations are collecting, transferring and consuming more PHI. More data drives more risk, and not of the garden variety; PHI is especially sensitive data that has the potential to cause significant harm to the patient or consumer and therefore draws the eye of more regulators.

Regulatory compliance and risk mitigation for data relationships as complicated as those faced by life sciences organizations is no simple task. Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) requirements was already complicated; now life sciences organizations are faced with more data to manage and protect, new regulations to consider and regulatory enforcement bodies that carry bigger sticks. For the COVID-19 emergency, regulatory focus shifted by necessity to the value side of the data coin, allowing for potentially non-compliant technologies to support the decentralized provision of care, but this relaxed stance will not last forever.[4] In order to continue to operate under a decentralized approach to care, organizations need to understand how to properly leverage technology innovations in a way that respects individual privacy rights, manages privacy risk and demonstrates regulatory compliance.

In order to continue to operate under a decentralized approach to care, organizations need to understand how to properly leverage technology innovations in a way that **respects individual privacy rights, manages privacy risk and demonstrates regulatory compliance**.

1 https://www.nejm.org/doi/10.1056/NEJMsr1503323

2 https://prahs.com/insights/covid-19-kicks-healthcare-technology-adaptation-into-high-gear

3 https://prahs.com/insights/wearable-technology-introduces-new-capabilities-to-clinical-trials

4 https://prahs.com/insights/covid-19-kicks-healthcare-technology-adaptation-into-high-gear

NEW TECHNOLOGIES

The rapid advancement of healthcare strategies would not be possible without the development of new and innovative technologies to support it. Surges in computing capability, lower storage costs, improved connectivity and mature data analytics have not only facilitated the development of digital health technologies, but also made them more accessible for widespread, decentralized use.

Mobile Medical Applications

Developers have taken advantage of mobile platform features to turn apps into medical devices or extensions thereof. 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.[5]

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 treatments, as well as provides the ability to monitor patient health status and behavior 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 PHI not only impact privacy rights, but may also impact patients' health if compromised.[6]

Artificial Intelligence (AI)

AI and machine learning technologies have the potential to accelerate research, development and the ability to diagnose and treat patients by deriving insights from the substantial amount of data generated through medical devices. These technologies are being used to identify patterns in medical records, images and genetic data and even make automated decisions based on these patterns.[7] However, the use of AI also presents a host of new legal and ethical concerns, such as how to regulate an algorithm and how to be transparent with data subjects when the "black box" of machine learning conceals why and how decisions are made and how those decisions impact them.

5 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5008929/

6 https://doi.org/10.1155/2018/5978636

7 https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device

DATA ACCOUNTABILITY

Under the current landscape of decentralized product and service provisions through remote and connected technologies, data may be **collected** at remote locations directly by patients, **transferred** to a clinical trial operator or healthcare provider, **sent onward** to trial sponsors or technology manufactures in identifiable or pseudonymous form and be **made available** to third-party service providers to facilitate care.

Under these circumstances, even well-meaning organization in the life sciences industry can have difficulty with the most basic questions of PHI privacy and governance: **who is responsible for protecting this data?**

While digital health technologies have the potential to advance the medical field, devices that monitor, measure and analyze various aspects of health and provide ready access to this information are raising questions on data privacy. Properly addressing these concerns will require life sciences organizations to understand the regulations surrounding these tools, their accountability under these regulations and how to address their legal requirements.

From a General Data Protection Regulation (GDPR) perspective, ultimate accountability for the data's management falls to the data's controller, the organization that determines the "purposes and means of processing" the data in question.[8] Every organization is a controller of their own data (think payroll processing or employee performance evaluation), but determining the controller of data collected from external data subjects can be more challenging. This is especially true for clinical trial data where the trial's sponsor, often formally the controller of the trial's data, may never see the data sets in identifiable form, only in the pseudonymous sets provided and maintained by the Contract Research Organization (CRO). This is a common point of confusion: pseudonymous data under most privacy regulations is not necessarily considered to be different than identifiable PHI, and never having received identifiable data sets does not absolve a trial sponsor (or any controller) from data protection and governance accountability.[9]

However, it is important to remember that regardless of specific designation of controller/processor/third party/service provider, any organization that has access to personal information, and PHI specifically, will have corresponding privacy responsibilities. Contract language with Standard Contractual Clauses or Data Protection Agreements will codify the requirements of all parties that interact with the data, often bringing standards for additional parties in line with those imposed upon controllers under GDPR. Each organization will need to protect their data, manage access to it, govern its use in accordance with the agreed-upon processing activities and prepare for and respond to breaches or incidents until that data is ultimately destroyed in accordance with retention requirements. While organizations across various industries rush to implement retention and disposition schedules to reduce their data risk, life sciences organizations must follow strict regulatory-driven retention guidelines, often preventing expedient disposal. Industry regulations, pharmacovigilance efforts and government reporting requirements all complicate the speedy disposal of PHI, making accountability for this data's protection and governance a long-term relationship. To alleviate these complications, life sciences organizations must not only know the full universe of the data they have and where they have it, but also know the scope of applicable data protection regulations to demonstrate that they are storing, managing and protecting that data appropriately.

8 GDPR Article 24 Section 1

9 GDPR Recital 26

USER-CENTRICITY:

Access to large quantities of high-quality data is necessary for advancing the medical field. However, the societal benefits of efficient and effective health solutions must be balanced with an individual's right to privacy.

Designing for the User Experience

Some privacy laws and regulations, such as the GDPR, require organizations to apply Privacy by Design and Privacy by Default principles in their data handling practices. This means that products, services and applications must be designed and developed to protect privacy as the default. Digital health strategies offer many benefits and privacy must be embedded into operations and technologies to protect the safety and confidentiality of patients and consumers. Ingraining privacy and security controls into product development and business operations sets organizations on a path to meet their privacy obligations to patients, consumers and regulators.

Meeting User Expectations

Although the enablement of new technologies and data sharing mechanisms has made health data easily accessible, using it for purposes other than that for which it was originally collected creates ethical and regulatory challenges. In general, organizations must obtain informed consent from the patient or consumer before using data for purposes other than direct patient care, public health or scientific research. While it is difficult to define all of the potential uses for data in the future, the uses must be consistent with what the patient agreed upon. Having security safeguards in place and removing identifiers from data through pseudonymization, anonymization and aggregation before it is used for secondary purposes may help reduce risk.[10]

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, monetization and breach of data can also threaten an organization's image of competence and trustworthiness. As organizations adopt new strategies and services, they need to be proactive and transparent about their data policies and practices to make consumers comfortable with sharing their data and reduce the likelihood of undermining the benefits that access to data may bring to the medical field.[11]

10 https://iapp.org/product/a191P000003oHFOQA2/a191P000003jnc7QAA/

11 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6628981/

CONCLUSION

Modern technology for collecting, transferring and processing data poses both an opportunity and a threat to organizations in the life sciences industry. Organizations can now reach consumers and patients more easily with their therapeutics, products, services and the care that they provide. But in order to do so, life sciences companies must wade into the risk-infested waters of PHI and address the obligations and regulations that come with it. When creating business strategies, leaders from life sciences companies should consider not just the value and opportunity associated with the data they obtain and utilize, but also the risks and requirements that are inherent to those strategies. Life sciences organizations must develop and maintain proactive and thoughtful data protection regimes that not only address existing data privacy regulations, but also consider future state, national and international legislation on the horizon.

People who know Life Sciences, know BDO.

www.bdo.com/**lifesciences**

CONTACT

KAREN SCHULER
Principal; Governance, Risk & Compliance National Practice Leader
301-354-2581 / kschuler@bdo.com

MARK ANTALIK
Managing Director; Data Privacy and Data Governance Services
617-378-3653 / mantalik@bdo.com

LANCE MINOR
Principal; Life Sciences National Co-Leader
301-354-0711 / lminor@bdo.com

TODD BERRY
Assurance Partner; Life Sciences National Co-Leader
617-239-4125 / tberry@bdo.com

ABOUT BDO LIFE SCIENCES

BDO's Life Sciences Practice provides the guidance that pharmaceutical, biotech, and medical device manufacturers need, when they need it. From understanding the complexities of research and development tax credits and FDA regulations, to licensing agreements and due diligence, we help our clients grow.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of skilled and committed professionals. The firm serves clients through more than 65 offices and over 740 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 91,000 people working out of over 1,600 offices across 167 countries.

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. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: 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.