JULY 2021
www.bdo.com/lifesciences

DATA PRIVACY AND GOVERNANCE CHECKLIST FOR LIFE SCIENCES

INSIGHTS FROM THE BDO LIFE SCIENCES PRACTICE

This checklist outlines the basics for understanding your current data protection posture regarding the **handling of consumer, patient, or other sensitive data**. Leverage the questions and responsibilities below to enhance your organization's privacy practices and reduce regulatory risk inherent to operating in the life sciences field.

Using this checklist, a life sciences organization will be able to:

Identify the data and regulations that will inform and impact a privacy program

Understand the level of risk posed by specific data interactions

Secure data from unauthorized access, use, alteration or disclosure

Support accountability and lifecycle management of data

Facilitate a user-centric approach to data protection

SCOPE

APPLICABLE REGULATIONS

Understand the data privacy regulations that apply to your organization, either as a result of the data you collect and use, or the jurisdictions in which you operate.

- ☐ **Does your organization need to be HIPAA compliant? How about GDPR? Maybe CCPA, CPRA, or the Virginia CDPA?**

DATA MAPS

Understand the different types of data your organization interacts with, where it comes from and to whom and to where it is traveling.

- ☐ **Does your organization maintain data maps or data flow diagrams to track patient/consumer data?**

DATA SUBJECTS

Be aware of individuals from whom your organization is collecting data. Understand the different laws, rights and protections associated with data from those individuals.

- ☐ **Does your organization understand how privacy rights differ among residents of different countries, patients/customers and your own employees?**

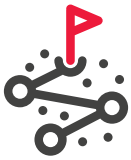
ASSESS

RISK ANALYSIS

Conduct regular risk assessments to understand the impact of starting a new project, standing up a new information system, setting up operations in a new country or onboarding a new service provider. Identify controls needed to mitigate these risks.

- ☐ **Is your new web application compliant with relevant data protection regulations covering the information it is collecting and the locations of the users?**

IMPACT ASSESSMENTS



Perform Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs) for new initiatives, operations, technology implementations and third-party relationships to identify potential privacy risks and measure the performance of mitigating controls.

- ☐ **Is your new technology compliant with your data privacy standards?**

RISK MITIGATION

Once identified, apply physical and technical safeguards and controls to reduce the data privacy risk associated with your organization's use of data.

- ☐ **How much security and privacy risk is your organization prepared to accept, and where are you exceeding that risk level?**

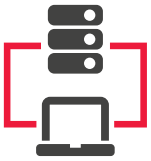
PROTECT

ENCRYPTION

Encrypt data both at rest and in transit to prevent unauthorized access or disclosure of personal data.

- ☐ **Is any of the personal data controlled or processed by your organization vulnerable to breach?**

BACKUP & RECOVERY



Prepare for events, incidents and disasters by maintaining regular backups and routinely stress test your breach response processes, procedures and technology. Create and test recovery plans to bring data and operations back online efficiently and effectively.

- ☐ **How long would it take your organization to identify, contain and address a data breach incident?**

ACCESS MANAGEMENT

Define a specific purpose for data before it is collected, use that data only for its intended purpose, and limit access to that data on a "need-to-know" basis to fulfil that purpose.

- ☐ **Has your organization increased its risk by allowing more people to access data than truly need it?**

GOVERN

RECORD OF PROCESSING ACTIVITIES

Keep detailed and current records of the systems on which your data is stored, the types of data stored on those systems, the sensitivity of that data, who is responsible for those systems, the retention cycle for the data, and activities your organization is conducting with the data it collects.

- ☐ **Do your organization's processing activities align to the consent provided by an individual for that data?**

DATA MINIMIZATION

Don't engage with more data than you need to. Limit your collection of data to only what is needed for a specific purpose, don't collect data "just in case" you might someday need it, and don't use the data for purposes other than that for which you collected it.

- ☐ **Do you truly need a consumer's Social Security Number to provide a service?**

DISCLOSURES/TRANSFER

Carefully address the processes, procedures and risks for data leaving your organization. Govern your data sharing practices in line with contracts and consent. Don't transfer data to an organization that won't protect it.

- ☐ **Are your service providers applying the same level of data protection and governance as your organization?**

ENABLE

NOTICE & CONSENT

Enable individuals to maintain and exercise control over their data through notice and consent practices. Enact straight-forward policies, written in plain language, to alert individuals as to what data your organization collects and why you are collecting it. Obtain the necessary consent for the purposes you disclose.

- ☐ **Do you use data from patients/consumers for a purpose for which they are not aware or have consented?**

PROCESS RESTRICTION

Respect an individual's right to limit the way your organization uses their data, as well as with whom you share their data.

- ☐ **Does your organization have a procedure in place to respond to an individual's request to restrict processing as required by applicable data privacy regulations?**

ACCESS & ERASURE

Develop procedures for individuals to request access to the data you hold about them, to obtain a copy of that data, and, if they so choose, to request that you delete their data.

- ☐ **If an individual requested that you delete their data, would you know all the locations where their data may be stored?**

HOW BDO CAN HELP

Need help managing your data and becoming compliant with the numerous existing and upcoming global data privacy regulations? BDO USA's Governance, Risk, and Compliance practice has deep experience supporting organizations in the life sciences industries navigate the complexities of data privacy risk mitigation and compliance. At BDO, we understand the unique data-related challenges in life sciences and will work closely with your organization to address compliance, while enabling you to derive maximum value from your data.

People who know Life Sciences, know BDO.

www.bdo.com/**lifesciences**

CONTACT

KAREN SCHULER
Principal, Governance, Risk and 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.