Global Privacy Policy

Effective: 17 June 2019

1. Introduction

Our purpose is clear and compelling: We are committed to *advancing the world of health*. In fulfilling our mission, we collect, process and use large quantities of Personal Data. We collect Personal Data (defined in Section 3) from customers, employees (referred to as "BD associates" under this policy), contractors, healthcare professionals, patients, business partners and others. We are committed to good stewardship of all Personal Data in our products, our internal systems and our day-to-day work. This Global Privacy Policy is an important part of our privacy framework that guides our work. BD takes data privacy seriously and believes that carrying out our business activities in compliance with applicable data protection laws and in accordance with sustainable corporate governance is fundamental to our business success.

1.1 Purpose

Doing business in a global economy requires Becton, Dickinson and Company, its divisions, and majority-owned or controlled subsidiaries ("BD", "we" or "our") to comply with a number of different laws and regulations related to privacy and data protection ("Data Protection Laws"). This policy sets forth enterprise-wide principles that govern all BD Processing of Personal Data (defined in Section 2) globally.

1.2 Scope & relevance

BD considers compliance with applicable Data Protection Laws and adherence to our ethical standards to be a fundamental principle of doing business globally. As a result, BD has established this policy setting forth the privacy and data protection principles, which BD will implement to ensure a general enterprise-wide standard for the collection, processing, disclosure and protection of Personal Data.

This policy applies to all BD divisions, departments and business units, and all BD associates, contractors, temporary workers, or outside consultants working on behalf of BD (together referred to as "Authorized Personnel").



1.3 Processing and applicable Data Protection Laws

This policy establishes a baseline set of principles that apply to any operation or set of operations performed using Personal Data, including accessing, collecting, recording, storing, organizing, structuring, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating, otherwise making available, safeguarding, aligning, combining, restricting, erasing, deleting or destroying (collectively "Processing"). Although this policy is global, individual regions, countries, states, provinces or other governmental bodies may impose additional and/or more restrictive principles or Data Protection Laws. BD departments or entities operating in or otherwise subject to the laws of those jurisdictions will comply with applicable Data Protection Laws. BD may implement additional policies applicable to those departments or jurisdictions (or regions) to manage compliance. If any applicable Data Protection Laws directly conflict with this policy or any supplementing policies, those Data Protection Laws govern any conflict with this policy.

Personal Data

The term "Personal Data" means any information that can be linked to an identified or identifiable person, which may include:

• Name, phone number, e-mail address, IP addresses, user name, log-in name or handle, passwords (clear text or hashed), date of birth, digitized or electronic signatures, Patient ID, and any other categories of Personal Data that BD determines may be covered by applicable Data Protection Laws.

The term "Personal Data" also covers certain categories of "sensitive" Personal Data that often receive additional protections and/or are subject to additional restrictions under Data Protection Laws. Such data may include:

- Social security number (or foreign equivalent), driver's license number, or other government issuedidentification number;
- Financial account numbers, and credit or debit card numbers (with or without any required security code, access code, personal identification number or password);
- Health information, including any information, that relates to: (i) the past, present, or future physical or mental health or condition of an individual, (ii) the provision of health care to an individual, or (iii) the past, present, or future payment for the provision of health care to an individual;
- Sex life or sexual orientation;
- Biometric information (e.g., fingerprint, facial recognition scan, retinal scan);
- Password;
- Criminal history or background;
- Race and ethnic origin (N.B. these attributes mean that photographs of individuals are also sensitive);
- Religion;
- Political affiliation; and
- Trade union membership.

3. Owner/data controller vs. service provider/data processor

BD collects and Processes Personal Data either as an owner/data controller or as a service provider/data processor. When acting as an owner/data controller, BD determines the means and purposes of Processing the Personal Data and BD is primarily responsible for ensuring compliance with applicable Data Protection Laws. When acting as a service provider/data processor, BD acts on behalf of a third party when collecting and

Page 2/8

Processing Personal Data. The principles set out in this policy may vary depending on whether BD is an owner/data controller or a service provider/data processor.

3.1 Owner/data controller

BD is typically acting as an owner/data controller, for example, when it collects and Processes the Personal Data of BD associates (in connection with their employment or engagement) or business partners (in connection with the business relationship) or when it collects and Processes Personal Data of patients to improve BD products and services.

3.2 Service provider/data processor

BD is typically a service provider/data processor when it provides services to customers, such as hospitals and health institutions, including providing medical devices, remote support, hosting services, and data analytic services. When acting as a service provider/data processor, BD shall ensure that the contract with the customer states that BD is acting as a data processor on behalf of the customer and that the customer is primarily responsible for ensuring compliance with applicable Data Protection Laws.

3.3 Service providers

BD may also engage third party service providers, including fulfilment partners, information technology vendors, hosting providers, and marketing providers. To the extent that such third parties are required to Process Personal Data in connection with their activities, these third party service providers will typically be considered service provider/data processors that are acting on behalf of BD. BD shall take all reasonable efforts to require third party service providers by contract to collect and Process Personal Data only on behalf of BD and to protect the Personal Data with appropriate security measures in accordance with applicable Data Protection Laws and this policy.

4. Global data protection principles

4.1 Transparency/notice

In its role as an owner/data controller, and in accordance with applicable data protection laws and regulations, BD will make available to individuals from whom, or about whom, Personal Data is collected, information about its policies and practices relating to the Processing of Personal Data, including what data is collected, how it will be processed (including to whom it may be disclosed and/or transferred), and contact information for submitting inquiries or complaints and any rights or choices available to individuals in connection with the Personal Data under the control of BD.

If BD is a service provider/data processor, this obligation rests with the BD customer.

4.2 Choice/control

In its role as an owner/data controller, BD will offer choices regarding collection and Processing of individuals' Personal Data where appropriate and make such choices readily available to individuals.

If BD is a service provider/data processor, BD will follow customer instructions on the choices and controls that BD must make available to individuals.

Page 3/8

4.3 Data minimization and retention

In its role as an owner/data controller, BD will only collect Personal Data to the extent that it is reasonably necessary and related to the purposes for which the Personal Data is obtained. In addition, BD may only retain Personal Data as long as needed for those purposes and as otherwise needed for further legitimate legal and business purposes, as outlined in applicable record retention policies.

If BD is a service provider/data processor, BD will follow the instruction of the customer with regard to collection and retention of Personal Data.

4.4 Processing, including disclosure

In its role as an owner/data controller, BD will limit Processing of Personal Data to uses reasonably expected by the individuals based on the nature of the relationship or context in which the Personal Data was collected. Disclosures of Personal Data to non-affiliated third parties will be limited to disclosures directly related to performing services on behalf of BD (e.g., service providers), as required or permitted by applicable law, and where third parties have executed appropriate data protection commitments with BD.

If BD is a service provider/data processor, BD Processes the Personal Data only for the purposes instructed by the customer and discloses the Personal Data only to authorized BD entities and third parties.

4.5 Access/accuracy

In its role as an owner/data controller, BD will provide individuals with reasonable access to their Personal Data upon request and satisfactory proof of identity and will respond to requests to correct or update Personal Data in a reasonable time and manner, as required under Data Protection Laws. If BD declines to provide access, it will provide reasons for declining to the individual.

In addition, BD will take reasonable steps to ensure that the Personal Data collected and Processed is accurate, and to keep the Personal Data up to date, where necessary.

If BD is a service provider/data processor, BD must follow the instructions of the applicable BD customer when receiving requests from individuals.

4.6 Security/safeguards

BD will take reasonable measures to protect Personal Data against loss, unauthorized access, use, destruction, modification or disclosure, appropriate to the level of risk and sensitivity of the Personal Data.

4.7 Data protection by design and by default

BD will implement appropriate technical and organizational measures to address the Global Data Protection Principles set forth in this Section 4, by design and by default in an effective manner, and to integrate the necessary safeguards into any uses or other Processing of Personal Data in accordance with applicable Data Protection Laws. These measures will take into account the state of the art (of the technology), the cost of implementation and the nature, scope, context and purposes of using Personal Data, as well as the risks posed by that use.

5. Personal Data incident or breach

Any BD associate who suspects or becomes aware of any unauthorized access to or disclosure of Personal Data is required to follow the applicable BD data incident or breach policy (or other guidance) identified on the Privacy, Product Security, and IT Information Security pages of Maxwell. Prompt notification is essential to BD taking the necessary steps to prevent further harm and to comply with Data Protection Laws. In the case of the General Data Protection Regulation, for example, BD is obligated to report its knowledge of a breach related to Personal Data within 72 hours of becoming aware of the breach.

Notification is essential to BD taking the necessary steps to prevent further harm and to comply with applicable Data Protection Laws, most of which have strict time limits for notifying government officials, affected individuals, and other parties.

6. Data protection training

All BD associates are required to complete applicable data protection training that is made available to them following their start date, and to complete all data security and privacy training provided thereafter. Specific departments that have access to Personal Data of BD associates, or of customers, patients or healthcare professionals, may receive additional training.

7. Data protection governance at BD

BD has established the following data protection governance structure relating to compliance with Data Protection Laws: Information Security Risk Council (ISRC), Chief Privacy Officer (CPO), Chief Information Security Officer (CISO), Data Protection Officer (DPO), Director Product Security/Product Security Officers, National Data Protection Coordinators (NDPCs), and business or technology owners of IT Systems.

8. Control review

The Chief Privacy Officer (CPO), working in conjunction with the Law Group or external consultants, Director of Product Security and/or the Chief Information Security Officer (CISO), will perform a periodic evaluation of specific controls against major legal, regulatory and policy requirements. The department, business unit, office, facility, country or region subject to review will be chosen based on a number of factors, including risk exposure. The purpose of periodic evaluation is to determine whether applicable controls are effective in managing the associated privacy and data protection risks and whether the requirements of this policy are being adhered to. The results of the periodic evaluation will be reported to BD leadership as required.

Questions

Any questions or comments relating to this policy and/or to Data Protection Laws may be directed to the local Data Protection Officer, a local National Data Protection Coordinator (NDPC) (where applicable), or the Chief Privacy Officer (CPO) at privacy@bd.com.

Page 5/8

10. Consequences of non-compliance

Any BD associate who fails to meet the standards and expectations of this policy or the Code of Conduct, may be subject to discipline. Such discipline shall be reasonably designed to deter wrongdoing and to promote compliance with this policy and the Code of Conduct, and may include without limitation, corrective actions up to, and including, termination of the individual's employment. Any contract with an individual who is not a BD associate or a legal entity that is asked to comply with this policy may be terminated by BD for a failure to abide by this policy, to the extent compatible with the terms of the relevant contract or applicable Data Protection Laws.

11. Obligation to report non-compliance

Except as prohibited by applicable law, BD associates have an obligation to report non-compliance with BD policy, both their own non-compliance or the non-compliance of another BD associate or a third party, to their supervisors, Human Resources, the Law Group and/or the Ethics & Compliance Department. The BD Ethics Helpline allows for anonymous reporting of non-compliance except to the extent such anonymous reporting is not allowed by law. You can reach the Ethics Helpline through the phone numbers or website identified on the Ethics & Compliance page on the BD Intranet, Maxwell. You can also report matters via email: ethicsoffice@bd.com.

12. Exceptions and changes

Exceptions will be granted only in very limited circumstances and with strong justification, where such exception is warranted under local law. Exceptions may only be approved by in advance by the Chief Privacy Officer. Exception requests must be sent to privacy@bd.com.

13. Updates

This policy may be updated by BD as required.

References

Code of Conduct

Approval

Author: Approver:

By: Frances Wiet By: Vincent A. Forlenza

Name: Name: Wincent a forling

Title: Vice President, Chief Privacy Officer

Ethics & Compliance

Title: Chairman and Chief Executive

Officer

Page 7/8

Revision log

Rev	Description of Changes	Changed By	Approved By	Date
2.0	Updated, incorporated into new policy design template and executed by CEO	Ethics & Compliance	Chief Executive Officer	6/17/19
1.0	New	Ethics & Compliance	Ethics & Compliance	5/23/18