Global Policy on the Protection of Personal Information

Effective Date: September 1, 2024
Revision Date: August 22, 2024
Version: 8
Approved by: Chief Ethics & Compliance Officer

Table of Contents

1. Objective

Bausch Health Companies ("Bausch Health" or the "Company") processes Personal Information to support our mission of improving people's lives through our healthcare products. We use Personal Information in our research and development, marketing of innovative products and in relation to our Associates. Bausch Health respects the privacy of persons who provide us with their Personal Information and complies with privacy laws and regulations from around the world.

This policy will provide standard principles governing the privacy rights of individuals who entrust their data to Bausch Health and the protection of Personal Information by Bausch Health, their affiliates, and third parties working on behalf of Bausch Health.

2. Scope and Applicability

In the course of our business, Bausch Health entities collect and use information relating to consumers, patients, healthcare professionals, employees, vendors, and others. This Policy covers all Personal Information collected, processed, handled, shared, used, and stored by Bausch Health.

This Policy applies to all employees, contractors, consultants and third parties who provide services on behalf of Bausch Health (collectively "Associates").

3. Definitions

"Anonymization" means the process by which Personal Information is irreversibly stripped of all identifiers and can no longer be linked back to the person. Once this process is done, it is no longer considered Personal Information.

"Data Privacy" generally means the ability of a person to determine for themselves when, how, and to what extent Personal Information about them is shared with or communicated to others.

"Personal Data Security Incident" means any incident that involves the permanent or temporary and accidental or unauthorized access, disclosure, modification, destruction, or loss of Personal Information transmitted, stored, or otherwise processed through Bausch Health Companies' Computer Systems or by any third party processing Personal Information on behalf of Bausch Health.

"Personal Information" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Pseudonymize" means replacing a person's name and most other identifying characteristics with a label, code, or other artificial identifiers to protect against identification of the person. Pseudonymized data is still considered Personal Information.

“Processing” refers to any operation or set of operations that are performed upon Personal Information, whether done by automatic means or otherwise. This includes the collection, handling, recording, organization, storage, updating or modification, retrieval, consultation, use, disclosure by transmission, dissemination or making available in any other form, linking, alignment or combination, blocking, erasure, or destruction of Personal Information.

“Sensitive Personal Information” means a subset of Personal Information that requires a higher level of protection. This may include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation, gender identity, social security or insurance information, criminal charges or convictions, national IDs or financial accounts including account numbers and personal identification numbers (PINs).

“Third Party” is any person, including a legal entity, with whom Bausch Health interacts and is not a Bausch Health company. For example, persons or businesses providing benefits administration, data aggregation, management administration, Customer Relationship Management (“CRM”) application providers, contract research organization and others.

4. Compliance with Law

4.1. This Policy is designed to set a uniform minimum standard with respect to the Company’s protection of Personal Information. Countries without Data Protection laws or those with a lower standard than set in this Policy shall comply with the minimum standards set forth in this Policy.

4.2. Various global laws are in effect that the Company must abide by with regards to business activities in all countries in which we operate. Company entities may implement local SOPs that meet local legal requirements and that support the principles of this Policy. When in conflict, the stronger of the requirements will apply.

4.3. All Associates are expected to recognize when they are Processing Personal Information and comply with the data protection requirements and principles that govern such data. Questions about compliance with local laws must be addressed to the Legal and Ethics & Compliance Department.

5. Applicable Privacy Regulations

The following is a non-exclusive list of applicable state, national and multinational privacy laws to which the Company adheres:

5.1. General Data Protection Regulations (“GDPR”)

5.1.1. A European Union (“EU”) law implemented May 25, 2018. GDPR requires organizations to safeguard Personal Information and uphold the privacy rights of all EU citizens. The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines.

5.2. Personal Information Protection Law of the People’s Republic of China (“PIPL”)

5.2.1. Passed on August 20, 2021, this law is formulated to protect Personal Information rights and interests, standardize Personal Information handling activities, and promote the rational use of Personal Information.

5.3. Personal Information Protection and Electronic Documents Act (“PIPEDA”)

5.3.1. Canadian regulation to support and promote electronic commerce by protecting Personal Information that is collected, used, or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act

5.4. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

5.4.1. HIPAA is the primary law in the United States imposing restrictions surrounding the use and handling of protected health information (“PHI). Among other things, HIPAA establishes the rules under which providers, insurance companies, other healthcare entities, and business associates can exchange information necessary for treatment, payment, and healthcare business operations.

5.5. Additional state-level privacy legislation in the United States, including laws in California, Colorado, Virginia, Utah, and numerous other jurisdictions.

5.5.1. Although HIPAA is the United States’ national legislation governing protected health information, various state laws have been enacted that impose additional requirements on the Company, including requirements pertaining to non-healthcare personal data. Each has its own elements, but there are similarities including rules for collection, processing, rights of data subjects, penalties, and fines, etc.

5.5.2. See the US Privacy Policy BHC-US-CMP-021, for further information about HIPAA and State Law compliance.

6. Policy and Principles

6.1. Lawful and Fair Processing of Personal Information

One of the fundamental principles of data privacy is that Personal Information should be processed in a lawful, transparent, and fair manner. All Associates must:

- Collect Personal Information only for a specified, relevant, and legitimate business purpose.
- Process Personal Information only with a legal justification to do so, such as when the individual has given his/her prior consent or when the processing is necessary to execute a contract, to comply with a legal obligation, or to pursue a legitimate and overriding business interest of Bausch Health.
- Provide a notice to individuals prior to collecting Personal Information about how their data will be used and shared, and include contact information in case of questions, enquiries, or complaints.
- Use Personal Information only as described in the privacy notice or consent form, or in a manner that any reasonable person would expect. Company shall not use Personal information incompatible with the purpose for which the Personal Information was collected.

6.2. Managing Personal Information: Proportionality, Integrity, and Retention

Bausch Health has an obligation to manage and maintain Personal Information in a responsible manner and in keeping with the expectations of individuals who entrust their Personal Information to Bausch Health. All Associates shall:

- Limit the processing of Personal Information to what is necessary and proportionate in light of the specified business purposes.
- Use reasonable means to keep Personal Information accurate, complete, up to-date and reliable for their intended use.
- Where required by law, maintain a centralized Record of Processing Operations (“RoPA”). The Record shall be made available to competent authorities upon request.
- Comply with the Company's data retention policies and retain Personal Information for only as long as needed to meet the legitimate business purposes for which the information was collected, and as required by applicable laws or regulations.
- Delete or render anonymous Personal Information that is no longer needed in a form that allows for the identification of the individual concerned.

- In the development and design phases of its Processing Operations, take into consideration and document the ability to meet the privacy principles set out in this policy.
- Comply with Bausch Health's security policies and procedures when processing Personal Information.
- Not share Personal Information with other Associates or third parties that do not have a valid business reason to access the information. For example, coded clinical trial data should not be shared with Marketing Associates.
- Report any Personal Data Security Incident to Information Technology ("IT") and the Ethics & Compliance Department immediately.

6.3. Individuals Rights – Choice and Access

The Company shall respect the rights which individuals have to access their Personal Information or request correction, amendment, or deletion of such data. In addition, individuals have the right to choose if their Personal Information is transferred to a third party or processed for a materially different purpose. Any decisions or requests received, shall be formally documented and actioned as a priority to the GDPR standard. The Company provides easily accessible methods for individuals to exercise their rights by proving a designated email address, provided in Section 12, and allocating responsibility to designated individuals who have the competency to fulfil all requests received. The Ethics & Compliance Department, in consultation with the Company's Data Protection Officer ("DPO"), will provide governance and have oversight of all requests and act as a point of escalation.

6.3.1. Choice

The Company will respect an individual's right to choose whether their Personal Information is:

- Disclosed to a third party or;
- Used for a purpose that is materially different from the purpose(s) for which it was originally collected.

During the course of the company's business operations, Bausch Health is required to disclose Personal Information to third parties. Prior to the disclosure of any Personal Information, Bausch Health will ensure the necessary contracts are agreed with the recipients and the nature and purpose of the processing is legitimate and lawful.

Bausch Health processes Personal Information for defined purposes in relation to the provision of services to customers, to comply with regulatory obligations and to meet contractual requirements. On this basis, Bausch Health does not process Personal Information for purposes that are incompatible with the original purpose for processing.

6.3.2 Access, Correction, Amendment or Deletion

The Company has implemented robust procedures for managing requests of this nature and provides a dedicated mailbox (Refer to Section 12) and resources to meet the expectations of the requester and ensure that Bausch Health fulfils its regulatory obligations.

6.4. Disclosures to Third Parties and other Bausch Health Affiliates

6.4.1. Bausch Health uses a variety of third-party service providers to support the delivery of our services to customers and to comply with contractual and regulatory obligations. Such service providers may include, without limitation, (a) professional advisors, auditors, and business partners, (b) vendors that provide cloud services, manage databases, perform analyses or data analytics, process payments, provide technical or customer support, or send communications on our behalf; and (c) companies with which we have promotional, marketing, advertising, or other commercial relationships, including financial institutions and companies that perform fulfillment and/or delivery services. These service providers are located globally, due to the international reach of our business. In each case, we take reasonable precautions to help protect Personal Information from unauthorized use or disclosure. For example, we conduct rigorous due diligence, enter into written agreements that commit such service providers to comply with all applicable data protection and privacy laws, keep information confidential and implement appropriate security measures with respect to such information. In addition, these service providers' access to Personal Information is limited to that necessary or advisable to perform tasks on our behalf. All agreements are based on Article 28 of the GDPR and include the data privacy principles, rights of audit, requirement to report security breaches and processing instructions. Certain laws may impose specific requirements as to the nature and language of the contractual guarantees. Where such requirements are mandatory, the Company will ensure the requirements are incorporated.

6.4.2. The Company may share Personal Information with other Bausch Health affiliates, government agencies and other third parties for legitimate business reasons, as required by law (including disclosures to law enforcement authorities in connection with their duties), to protect the interests of the Company, or with the authorization of the individual concerned.

6.4.3. Personal Information Disclosure in Response to Lawful Requests by Public Authorities

Bausch Health will not disclose any Personal Information unless expressly permitted by contractual terms, except where it is necessary to comply with applicable laws and regulations or a valid and binding order of a law enforcement agency, such as a subpoena or court order.

Bausch Health is not a likely routine target for US surveillance matters, due to the nature of our data processing activities. The Company would not provide any public authority with direct or unlimited access to our customers' data. We also agree not to provide access to our encryption keys. Requests for data access must comply with applicable legal requirements and procedures and must be reviewed by the Bausch Health Legal team.

Company agrees to promptly notify the data exporter if we have reason to believe that we have become the subject of laws or practices.

We agree to promptly notify the data exporter and where possible and when acceptable to the data exporter, the individuals concerned, if Bausch Health receives a legally binding request from a public authority, including a judicial authority, for the disclosure of Personal Information transferred pursuant to the EU – US DPF, or becomes aware of any direct access by public authorities to Personal Information transferred pursuant to the EU – US DPF.

If we are prohibited from notifying the data exporter and/or the individuals concerned under US law, Bausch Health will endeavor to obtain a waiver of the prohibition as soon as reasonably possible. We will document our endeavors and if required, provide on request to the data exporter. Company will then provide notice as soon as possible after a legal prohibition has been revoked as permitted by applicable orders or laws.

6.5. Transfers Across Borders

As a global company, Bausch Health may transfer Personal Information among its affiliates and with third parties who support our business. These transfers in many instances will require the transfer of data across country borders. Data protection laws in many jurisdictions have specific requirements to legally send data outside their country's borders. These requirements apply not only to transfers to and from third parties but transfers between and among Bausch Health legal entities.

Each country with specific laws and restrictions on data transfers will implement SOPs governing these transfers.

All Associates involved in business activities that require the transfer Personal Information outside of their country must:

- Determine if they have a legitimate justification for the transfer of Personal Information
- Follow any local SOPs and legal requirements prior to transferring Personal Information
- If managing a global system, consult with the Global Privacy Office for global requirements

6.5.1 Onward Transfers to third parties

Bausch Health understands and accepts the potential risk and liability when our third parties engage another organization to undertake data processing activities on behalf of Bausch Health involving the onward transfer of Personal Information. The Company applies measures for managing associated risk and liabilities by ensuring contract terms, which are equivalent or no less onerous than the Bausch Health terms imposed on those organizations. Where the other organizations fail to fulfill their contractual obligations, the third party shall remain fully liable to the Company for the act or omission of the other organization.

6.6 Investigatory and enforcement powers of the Federal Trade Commission

Should Bausch Health be subject to a court order that is based on non-compliance or an order from the Federal Trade Commission (“FTC”) that is based on non-compliance, the Company shall make public any relevant EU-US DPF related sections of any compliance or assessment report submitted to the court or FTC to the extent consistent with confidentiality requirements.

The Federal Trade Commission Act is the primary statute of the Commission. Under this Act, as amended, the Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establish requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public.

The FTC has enforcement powers and can issue warning letters to warn companies that their conduct is likely unlawful and that they can face serious legal consequences, such as a federal lawsuit, if they do not immediately cease the conduct.

The Commission can obtain penalties against a company that acted unfairly or deceptively through the Penalty Offense Authority. Under this authority, the

Commission can seek civil penalties if it proves that (1) the company knew the conduct was unfair or deceptive in violation of the FTC Act and (2) the FTC had already issued a written decision (see below) that such conduct is unfair or deceptive.

6.7 Binding Arbitration

Provided that an individual has invoked binding arbitration by delivering notice to Bausch Health, the Company accepts its responsibility to arbitrate claims pursuant to the Recourse, Enforcement and Liability Principle and follow the terms as set forth in Annex I of the DPF Principles,

On receipt of any claims raising concerns of the Company violating its obligations under the DPF Principles, Bausch Health is committed to determining whether any such violation remains fully or partially unremedied. With respect to the claimant, the Company will support the Binding Arbitration Mechanism to ensure the necessary remedies are determined and facilitate non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question).

The Company has registered with The International Centre for Dispute Resolution®-American Arbitration Association® (ICDR-AAA®) and contributes to cover the arbitral costs, including arbitrator fees, up to maximum amounts.

For more information on Binding Arbitration Mechanism for individuals in EU/EEA and UK (or Gibraltar) refer to; https://go.adr.org/dpfeufiling.html

6.8 Security

Bausch Health shall implement appropriate administrative, technical, and physical measures to safeguard and appropriately protect Personal Information from unauthorized use, disclosure, loss, destruction, and alteration. Such safeguards will take into account the state of the art and sensitivity of the Personal Information concerned. The particular risks that are presented by the processing activity must be evaluated to assess the appropriate level of security required.

Bausch Health shall maintain a process to report data security breaches, investigate such breaches, and report as required by local law. The Company shall maintain a record of data breaches that will be made available to competent regulatory authorities upon request.

7. Data Privacy Governance

Bausch Health shall maintain a data privacy program and governance structure to oversee global data privacy requirements and update management on the legal environment, status of the program and any associated risks. The privacy governance structure is comprised of:

- A Global Data Privacy representative responsible for the oversight and implementation of the Company's Data Privacy and Protection program, in conjunction with a third-party Data Privacy Officer (“DPO”).
- In some instances, the DPO may be required by law. In these cases, the DPO will be assigned and carry out the responsibilities as described in the law.
- Regional Compliance Officers (“RCOs”) who are responsible for oversight and implementation of the Company's Data Privacy and Protection program at the regional/country level. The RCOs provide guidance to the region on data privacy requirements and will be consulted on important projects affecting the processing of Personal Information. The RCOs are the contact point for interactions with Government Authorities.
- Senior Management IT Security is responsible for establishing and maintaining a Company-wide IT systems security program to ensure electronic information assets are adequately protected. Information security representation on steering committees is recommended.

8. Monitoring

Bausch Health conducts regular, periodic auditing and monitoring of its activities. The Ethics & Compliance department maintains an annual monitoring plan including activities associated with the handling and processing of Personal Information. Monitoring is documented and corrective and/or preventive actions are applied as warranted.

9. Training and Education

Bausch Health provides training to all Associates on this Policy and Data Privacy and Protection principles. Tailored training is delivered to Associates whose roles involve the handling and processing of Personal Information at regular intervals. Additional education is provided to Associates in the form of various Communications tools, including Ethics & Compliance newsletters.

10. Consequences of Violations

Associates and consultants who fail to comply with this Policy may be subject to appropriate discipline and sanction, up to and including termination of employment or contract.

11. Policy Maintenance

The Ethics & Compliance department is responsible for publishing and maintaining this Policy. The Policy will be reviewed and revised on a routine basis, and/or as needed to accommodate Privacy legislation changes. The business units and applicable functions are responsible for implementing appropriate SOPs and ensuring compliance with this Policy and associated procedures.

12. Questions

Any questions, concerns or suspected violations of this Policy should be directed to your manager, the Ethics & Compliance Department, the Legal Department, or the Bausch Health Ethics Hotline (http://hotline.bauschhealth.com/)). Inquiries may also be sent to Privacy@bauschhealth.com.