Global Policy on the Protection of Personal Information

Effective Date: March 1, 2020
Revision Date: May 19, 2023
Version: 4
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.

"Data Privacy Breach" means any unauthorized disclosure, acquisition, access, destruction, or alteration of, or any similar action involving Personal Information, or any other incident where the confidentiality of Personal Information may have been compromised.

"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. The Company recognizes that certain laws may impose stronger requirements than those described in this Policy. Company entities shall provide information in the form of local SOPs that meet local legal requirements and support 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. Policy and Principals

5.1. 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.

5.2. 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, the Company must maintain a centralized Record of Processing Operations. 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.
- Where Personal Information is no longer needed in a form that allows for the identification of the individual concerned, the Personal Information shall be deleted or rendered anonymous.
- In the development and design phases of its Processing Operations, the Company shall 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 Data Privacy Breach to IT, the Ethics & Compliance Department, or to your local Data Privacy Representative.

5.3. Rights of Individuals

Company shall consider requests made by individuals for access, rectification, restriction, opposition, erasure, portability and not to be subjected to automated decision-making, and shall comply with such requests where required by law. Where these laws are in effect, the local Data Privacy Representative and/or Ethics & Compliance Department will provide a Standard Operating Procedure detailing the specific requirements in that country.

5.4. Disclosures to Third Parties and other Bausch Health Affiliates

5.4.1. 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.

5.4.2. The Company may disclose Personal Information to third parties provided it puts in place contractual guarantees that require the Third Party to have at least the same level of privacy and security protection to the Personal Information as Bausch Health. All agreements must include the data privacy principles, rights of audit, requirement to report security breaches and processing instructions.

5.5. Transfers Across Borders

As a global company, Bausch Health may need to 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 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 that transfer of Personal Information outside of their country must:

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

5.6. Security

Bausch Health shall establish 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 establish and 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.

6. Data Privacy Governance

Bausch Health will establish 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 shall be comprised of:

- A region/country Data Privacy Representative (“DPR”) who is responsible for the oversight and implementation of the Company's Data Privacy and Protection program within that country/region and provide guidance on data privacy requirements. The DPR will be consulted on important projects affecting the Processing of Personal Information and is the contact point for interactions with Government Authorities.
- A region/country privacy council made up of representatives from the various departments and business units. This committee will be responsible for working with the DPR to coordinate the implementation of the program within their departments and business units.
- In some instances, a Data Privacy Officer (“DPO”) may be required by law. In these cases, the DPO will be assigned and carry out the responsibilities as described in the law. The appointment of a DPO does not remove the requirement for region/country level DPRs and a region/country level privacy steering committee. 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.

7. 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.

8. Training and Education

Bausch Health provides training to all Associates on this Policy. 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.

9. Consequences of Violations

Directors, employees, temporary staff, 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.

10. Policy Maintenance

Corporate Ethics & Compliance is responsible for publishing and maintaining this Policy. The business units and applicable functions are responsible for implementing appropriate SOPs and ensuring compliance with this Policy and associated procedures.

11. 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 EthicsPoint Hotline. Inquiries may also be sent to Privacy@bauschhealth.com.

12. Review and Approval

This Global policy has been approved by:

David Alexander
Chief Ethics & Compliance Officer