A. PURPOSE

In the regular course of business, Baxter Healthcare Ltd. ("Baxter") acquires Personal Information by interaction and communication with patients, healthcare professional, employees, and others. Baxter recognizes and respects the privacy rights of individuals with regards to such Personal Information. As evidence of its commitment to privacy, Baxter's management has established this Policy and Baxter's Global Privacy Program, to ensure that respect for privacy is a key part of Baxter company culture and operations.

This Privacy Policy is designed to accomplish the following objectives:

- Increase awareness of UK legal requirements for handling and protecting Personal Information;
- Set forth a clear and comprehensive policy for handling Personal Information;
- Establish accountability for all individuals who handle Personal Information; and
- Enable Baxter to meet business, legal, and regulatory responsibilities relating to Personal Information.

The UK policy is aligned with Baxter's Global Privacy Policy as well as those of the UK Data Protection Act 1998 (DPA).

B. SCOPE AND APPLICABILITY

This Policy establishes a minimum standard within Baxter UK for collecting, using and protecting Personal Information. It covers any Personal Information that is collected, stored, processed, or transferred in electronic or paper form in connection with Baxter's business operations, such as information from patients, health care professionals (e.g., physicians, pharmacists, and nurses), employees or third party business associates.

This Policy must be implemented and followed in all Baxter businesses and functions in the UK.

Personal Information is not to be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection or the explicit consent has been obtained from the individual to whom the Personal Information relates, Personal Information relating to UK patients, health care professionals, employees or third party business associates may be transferred to Baxter business units in the United States as Baxter participates in the International Safe Harbor Program. Personal Information may also be transferred to Switzerland as this country provides adequate protection under its local laws. Personal Information may be transferred to Baxter India Private Limited as this organisation is contractually obliged to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. Information which may be transferred to Baxter India Private Limited for employees, applicants, former employees, beneficiaries, dependents, emergency contacts, and contract workers includes name, job title, business unit, business address, business telephone number, business email address, salary and compensation information, stock option information, benefits enrolment and related information (but no medical information), and evaluative and job performance information. The Personal Data transferred will not concern any special or sensitive categories of data.

Baxter business units in the United States must always follow the Safe Harbor Privacy Principles, which may be more detailed than corresponding provisions of this Policy, in handling Personal Information transferred from the UK to the United States. Baxter business units in the United States will comply with the Global Privacy Policy. It is possible for personal data to be transferred to additional counties once it has been determined that they provide a suitable level of protection. In such an event this policy will be updated.

For further information related to UK employees, reference can also be made to the Baxter Employee Privacy Principals.

This Policy is to be followed not only internally, but also by all Baxter agents, temporary staff, contractors, service providers and consultants in their handling and processing of Personal Information on behalf of Baxter. Any Third Party in receipt of Personal Information shall be responsible for ensuring suitable policy awareness training is implemented and managed.

As of the effective date, this Policy replaces and supersedes the former Baxter UK Data Protection Policy All Personal Information must be handled and protected according to the requirements set forth in this Policy, subject to the circumstances described under the Exceptions (Section Q) of this Policy.

C. DEFINITIONS

TERM	DEFINITION
Baxter's Global Privacy Program	The global privacy compliance program approved by Baxter's Corporate Responsibility Office.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Country General Management	Senior Baxter leadership in the respective country / organization.
Data Privacy	The legal rights and expectations of individuals to control how their Personal Information is collected and used.
Data Protection Act (DPA)	The UK Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. It implements the requirements of the EU Data Protection Directive (95/46/EC).
Data Protection Authority	Governmental agency responsible for the enforcement and interpretation of local privacy laws and regulations. In the UK this is the Information Commission.
Data Quality	The accuracy, completeness and relevancy of information.
Explicit Consent	Agreement by an individual, demonstrated by an observable or affirmative act, whether in writing, orally or by some other means.
Global Information Security Officer (GISO)	IT Director responsible for Information Security strategy and activities throughout the Global Baxter organization. Refer to the Global Information Protection Policy for more information regarding this role.
Global Policy	A set of rules applicable to all business, regional and functional units or domains that must be adhered to by all persons accountable to these domains. Specific policies may be adapted to enable scalability and flexibility.

Global Privacy Officer (GPO)	Corporate Counsel responsible for Data Privacy strategy and activities throughout the Global Baxter organization. Refer to the Global Information Protection Policy for more information regarding this role.
Implicit Consent	Agreement by an individual, inferred from the context or by the inaction of the individual.
Information Commissioner's Office (ICO)	UK independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Security	The means of ensuring that data and/or information is protected from corruption (Integrity), destruction (Availability), and/or disclosure (Confidentiality)
Local Privacy Owner (LPO)	Individual Baxter employees who are responsible for the implementation and ongoing compliance with this Policy. They also serve as point of contact for privacy-related questions and issues.
Personal Information	Personal data is information which relates to an individual who can be identified from that information, whether or not in conjunction with any other information. Common examples of personal data which may be used by Baxter in its day to day business include names, addresses, telephone numbers and other contact details, CVs, performance reviews, salaries and statements of opinion or intention regarding individuals.
Processing	Any operation or set of operations which is performed upon Personal Information, for example, Baxter will be processing personal data if it holds personal data and/or carries out any operation relating to that information such as altering or deleting it, accessing, downloading, reviewing or transferring it.
Sensitive Personal Information	personal data consisting of information as to • the racial or ethnic origin of the data subject, • his political opinions, • his religious beliefs or other beliefs of a similar nature, • whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), • his physical or mental health or condition, • his sexual life, • the commission or alleged commission by him of any offence, or • any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such

	proceedings.
Standard	Derived from generally accepted industry standard frameworks, a specific set of rules that are designed to structure and guide implementation of policy and allow an organization to operate uniformly and effectively; a set of auditable minimum requirements that support policy objectives.
Third Party	An entity that is independent and legally distinct from Baxter or any of its businesses or subsidiary companies. [**Note: the safe harbour principles' definition of "third party," includes *both* unaffiliated companies and companies affiliated by common ownership. However, it does not apply when a disclosure is made to a third party performing a task on behalf of the US entity**]

D. POLICY

1.0 Management

To establish a comprehensive privacy program, Baxter has adopted internationally-accepted principles of fair information practice as the basis for this Policy. These principles are aligned with concepts and requirements from the European Union's Data Protection Directive (95/46/EC) and the U.S. Department of Commerce's International Safe Harbor Privacy Principles. They also follow the framework of the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP) and comply specifically with the UK Data Protection Act 1998.

2.0 Notice

Baxter must notify individuals about the purposes for which it collects, processes, stores and/or discloses information about them. Notice must be communicated in a clear and easy-to-understand manner.

At a minimum, the Notice statement must contain (unless it is evident from the context):

- The type of information that is collected;
- The purpose for which the information is collected;
- If there is a legal requirement to collect the information, a statement of this fact;
- How the information will be used or processed;
- The choices and means Baxter offers individuals for limiting its use and disclosure
- If the information will be collected by or disclosed to third parties, a statement of this fact and the purposes for doing so;
- How individuals can access their information and correct or delete it if it is inaccurate; and
- How to contact Baxter with questions, corrections, complaints, and disputes.

Where feasible, Baxter must provide the Notice to an individual at or before the time of the collection of Personal Information and also before Baxter uses such information for a purpose other than that for which it was originally collected or processed or discloses it for the first time to a Third Party.

3.0 Choice and Consent

Baxter must obtain consent from individuals when required or appropriate. Baxter also must offer individuals the opportunity to choose (opt-out), and clearly communicate any such choices available to such individuals, when (a) Personal Information is collected or used by a Third Party, or disclosed by Baxter to any such Third Party; or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorised by the individual.

For Sensitive Personal Information, unless an exemption applies, the individual must be given affirmative or explicit (opt-in) choice if the information is to be disclosed to a Third Party or used for a purpose other than those for which it was originally collected or subsequently authorised by the individual through the exercise of opt in choice.
[***Note: there are exceptions to this e.g., to establish legal claims or defences; to provide medical care; and to carry out employment law obligations***]

Specifically, when consent is required or appropriate, Baxter must:

- Request the consent of the individual using the type of consent (opt-out or opt-in) that is required or appropriate;
- Ensure that the choices provided to an individual are complete and clear (e.g., how to "opt-out");
- Inform individuals of the consequences for failing to consent or to provide their information;
- Inform individuals regarding how they can change their consent decisions, if this is feasible;

- Verify that Baxter's use of individual Personal Information is consistent with consent obtained; and
- Obtain new consent if Personal Information will be used for a purpose other than originally disclosed to the individual.

Consent must be obtained in accordance with the DPA and in line with any relevant guidance published by the Information Commissioner.

4.0 Collection

Baxter must collect or obtain Personal Information only in a fair and lawful manner.

Specifically, Baxter must:

- Collect only as much Personal Information as is required by law or needed for the purposes about which the individual has been informed;
- Collect Personal Information in a fair and non-deceptive manner;
- Clearly indicate to individuals which Personal Information is required to be disclosed and which is optional at the time of collection;
- Collect Personal Information from individuals consistent with the DPA;
- Collect Personal Information directly from the individual, when possible; and
- Verify that Personal Information collected from third parties is reliable and legally obtained.

5.0 Use and Retention

Baxter must use, process, store, and/or retain Personal Information only for legitimate business purposes or as authorized by the individual.

Specifically, Baxter will use, store, and/or process Personal Information consistent with:

- Stated purposes for which it was collected;
- Consent obtained from the individual; and
- Contractual, regulatory, and UK laws and requirements.

Personal Information must be retained and destroyed according to applicable Baxter data retention policies and procedures.

6.0 Access

Baxter must provide individuals about whom it processes Personal Information an opportunity to access and correct their information.

Specifically, Baxter must provide a:

- Response to the request for access to Personal Information in a timely manner, in a format convenient for both Baxter and the individual; and
  Chance for an individual to review its Personal Information, challenge its accuracy, and have it corrected, amended or deleted.

Baxter must authenticate individuals before allowing access to or providing Personal Information. Access to Personal Information may be denied if an unreasonable request is made (e.g., requests that do not follow the procedure outlined in the privacy Notice or requests which would provide Personal Information about others besides the requesting individual). However, in cases in which access is denied, Baxter must provide a reason to the individual and a point of contact for further inquiry.

7.0 Disclosure and Onward Transfer

Baxter may share an individual's Personal Information with Third Parties as required for normal business operations, including providing services and products to patients, health care professionals (e.g., physicians, pharmacists, and nurses) and employees.

When disclosing information Baxter must:

- Only disclose Personal Information to Third Parties for the purposes identified in the Notice provided to individuals;
- Verify that Baxter's actions align with the consent provided by the individual, in addition to any legal and/or regulatory requirements;
- Require Third Parties, through contractual clauses and/or written agreements to adhere to a baseline of privacy and information security controls – as approved by the respective legal team; and
- Require Third Parties to process Personal Information in accordance with the individuals' choices and consent.

The Baxter director, officer, employee, or contractor responsible for each Third Party relationship is responsible to ensure compliance with this Policy by such Third Party.

Personal Data relating to UK patients, health care professionals, employees or third party business associates may be transferred to Baxter business units in the U.S.

8.0 Security

Baxter takes reasonable precautions, including administrative, technical, personnel, and physical measures, to safeguard Personal Information against loss, misuse and unauthorized access, disclosure, alteration, destruction, and theft.

Please refer to the Global Information Classification Policy and Global Acceptable Use of Information and Technology Policy for more information regarding Baxter's established security requirements, controls, and practices.

9.0 Data Integrity and Data Quality

Baxter must employ reasonable processes to keep Personal Information accurate, complete, and up-to-date for the purposes for which it was collected.

Specifically, Baxter must:

- Implement procedures to keep Personal Information reliable for its intended use, as accurate, complete and up-to-date as needed; and
- Except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated, , allow and encourage individuals to keep their Personal Information accurate, complete and up-to-date.

10.0 Monitoring and Enforcement

Baxter is committed to monitoring and enforcing ongoing compliance with this Policy and with applicable privacy laws, regulations and obligations. The Global Privacy Officer is responsible for working with Baxter's legal staff to ensure such compliance.

Specifically, Baxter must:

- Inform employees, customers, or patients with questions, concerns, or complaints about Baxter's privacy practices as to how they can contact Baxter.

For enquiries originating in the UK, individuals may submit a question or complaint to the UK LPO at UK_SHS_ Data_ Privacy@baxter.com , or via Baxter's Global Ethics & Compliance Helpline at: www.baxter.com/compliance;

Enquiries may also be submitted through Baxter's on-line Global Privacy Complaint Form at: https://www.baxter.com/information/privacy/privacy_feedback.html;

- Acknowledge, formally document, investigate, address and respond in a timely manner to formal complaints that are received.

- Provide a readily available and affordable independent dispute resolution mechanism to handle complaints not resolved to the individual's satisfaction by working if necessary with the ICO to resolve the complaint.

- Include conformance to provisions of this Policy in certain standard audits of company operations involving Personal Information.

- Perform periodic privacy compliance assessments of Baxter´s internal practices to ensure that they conform to this Policy and related standards, as well as to applicable privacy laws, regulations and obligations.

Any and all potential, apparent or actual violations of this Policy must be immediately reported to the Local and Global Privacy Officers.

11.0 Consequences of Non-Compliance

All Baxter directors, officers, employees, agents and contractors are expected to fully comply with this Policy. Violations of this Policy will be investigated and remediated. Failure to comply with this Policy may result in disciplinary action up to and including termination of employment or contract.

The Global Privacy Officer must approve exemptions from adherence to particular provisions of this Policy. Exemptions to this Policy will only be considered if special circumstances do not allow for the practical implementation of a requirement, if a UK or European law or regulation supports a requested exemption, and if there are compensating controls in place to mitigate the risk.

12.0 Exceptions

Under certain limited or exceptional circumstances, Baxter may, as permitted or required by applicable laws and obligations, process Personal Information without providing notice or seeking consent. Examples of such circumstances include investigation of specific allegations of wrongdoing or criminal activity; protecting employees, the public or Baxter from harm or wrongdoing; cooperating with law enforcement agencies; auditing financial results or compliance activities; responding to legal requirements or process; meeting legal or insurance requirements or defending legal claims or interests; satisfying employment laws or agreements or other legal obligations; collecting debts; protecting Baxter's information assets; in emergency situations, when vital interests of the individual, such as life or health, are at stake; succession planning; business re-organisation; and in cases of business necessity.

In addition, Baxter may, as permitted or required by applicable law and obligations, process Personal Information without providing access, such as in the circumstances described above; when the privacy

interests of others would be jeopardised; or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy.

13.0 Ownership and Responsibilities

The Baxter Operating Committee is primarily responsible for implementing controls throughout the organization, consistent with the Baxter Code of Conduct. The Baxter Operating Committee acknowledges and supports the strategic importance of data privacy across Baxter. The Operating Committee also recognizes the importance of an effective data privacy program across Baxter to the success of the enterprise.

The Global Privacy Officer (GPO) and Global Information Security Officer (GISO) are given responsibility for establishing and managing an information privacy and security governance function, and through corporate governance structures, enforcing adherence to the prescribed Global Policies, principles and standards.

The Global Privacy Officer (GPO) is responsible for ensuring that the privacy guidelines, programs, procedures, training, and other measures necessary to implement this Policy are developed and put into practice.

Baxter UK General Management is responsible and accountable for the preparation and the content of the local privacy policy.

The UK LPO is responsible for the implementation, communication and ongoing compliance with the local country privacy policy. The LPO is also the local point of contact for questions and issues related to this Policy which will be considered in cooperation with the UK Corporate Counsel. Contact can be made via email in the first instance - UK_SHS_Data_Privacy@baxter.com .

15.0 Periodic Revision Schedule

This Policy will be reviewed and modified, as necessary, by the UK LPO and UK Corporate Council, at least every two years.

E. REFERENCES AND ASSOCIATED DOCUMENTS

This Policy should be read in conjunction with corporate policies that set forth Baxter's expectations for the behaviors of directors, officers, employees, agents and contractors. Those policies include the following:

Global Privacy Policy
Global Information Protection Policy
Global Acceptable Use on Information and Technology Policy
Baxter Employee Privacy Principals

F. CHANGE HISTORY

VERSION	CHANGE
1.0	New Policy in line with Corporate Policy CP-IP-03 version 1.0
2	Addition of provision for transfer of data to India – section B

3.0	Change of LPO details