DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Global Privacy Policy – General Data Protection Regulation
PAGE: 1 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: May 25, 2018	**REFERENCE NUMBER:** IP.GEN.005
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities and business units who are:

1. Established in the European Union (EU) and process information relating to an identified or identifiable natural person (Personal Data), as defined below; or
2. Established outside the EU and offers goods or services to residents of the EU and/or monitors their behaviour.

This Policy also applies to any company or individual who provides goods or services to any of the companies captured by the criteria above where Personal Data is Processed.

PURPOSE: To establish Company policy (in all territories worldwide) for compliance with the General Data Protection Regulation (GDPR), 2016 and any other applicable Data Protection Laws.

POLICY:

1. The Company will Process Personal Data lawfully, fairly and in a transparent manner.
2. The Company's International Division (HCA International Limited) will maintain appropriate Data Controller registration(s) with the Information Commissioner's Office (ICO) as required by the Data Protection Laws.
3. Business Owners will only collect Personal Data for specified and legitimate purposes. Once the purpose of collection is determined, the Company will not Process further such Personal Data in a manner that is incompatible with those purposes.
4. If a Business Owner has a need for further Processing of Personal Data that is incompatible with the original collection purpose, the Business Owner is required to submit a formal request to the Data Protection Officer (DPO) for approval. If approved, the DPO will document this additional purpose (and any additional procedures to be followed) in the record of Processing documentation.
5. The Company will implement measures and procedures, as necessary, which minimize the Processing of Personal Data to that which is adequate, relevant and limited to what is necessary for the specified purposes.
6. The Company will securely destroy data which is no longer necessary for the purposes for which it was collected, except as required by law or any other applicable regulations and guidance relating to the healthcare sector.
7. The Company will ensure that Personal Data is accurate and, where necessary, kept up to date.
8. The Company will ensure that appropriate technical and operational measures are in place to ensure the integrity, availability and confidentiality of Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

Governance and Accountability for GDPR Compliance

A: Information Governance Board

The Company maintains an Information Governance Board (IGB) comprising of senior Executives of the Company and the Data Protection Officer (DPO). The IGB, in accordance with its terms of reference, is responsible for ensuring that:

a. Personal Data is Processed in accordance with the Data Protection Laws;
b. An appropriate privacy governance framework is in place;
c. Appropriate technical and organisational measures are put in place to keep Personal Data secure; and
d. Data Subjects' rights are upheld.

B: Managers and staff

1. All managers/supervisors are directly responsible for ensuring that their team members comply with this Policy and the associated Data Protection Standards.
2. All managers/supervisors will make workforce members aware that failure to comply may lead to disciplinary and/or legal action against company personnel or third parties that may result in dismissal, breach of contract claims, and civil or criminal prosecution.
3. The Company will provide training to personnel who are involved in any Processing of Personal Data. All Personnel must annually affirm their understanding of, and acceptance to abide by, this Policy and associated Data Protection Standards. All Personnel must undertake approved Data Protection Training on an annual basis or more frequently if required.
4. Third Parties, Embassies, Agents and Company entities located outside of the United Kingdom (UK) must notify the DPO of any changes in their circumstances that might impact the Company's current or future compliance to Data Protection Laws.

C: Data Protection Officer

1. The Company will appoint a dedicated DPO who will monitor compliance with the Data Protection laws and provide advice to the IGB and Personnel. The DPO will be the independent contact point for the relevant Supervisory Authority and Data Subjects who are exercising their rights or who have concerns over how their Personal Data is being Processed.
2. The Company will ensure the DPO is able to perform their tasks in an independent manner without instructions to achieve any desired outcome.
3. The DPO will not be unfairly penalised or dismissed for performing his or her tasks.

D: Data Processing and Transfer

1. The Company will ensure that data transfers within the Company are covered by the Intra-Group data transfer agreement which is based on the provisions of the EU Commission Model Clauses.
2. If the Company determines that a data transfer to third parties is necessary and permissible, the Business Owner is responsible for completing a due diligence exercise to ensure that the minimum amount of Personal Data is transferred and that all parties involved in the Processing of Data have appropriate technical and organisational measures in place to ensure that Personal Data is kept secure.
3. The Company will consider privacy risks and remediation plans for those risks at the outset of new projects and when looking at mergers or acquisitions, taking into consideration the privacy risks to Data Subjects.

Definitions:

Where this policy is being applied in the US, please refer to the Information Security Common Terminology document for definitions. See also the Information Protection Patient Privacy Policies (IP.PRI) for definitions applicable to data breaches in scope for HIPAA/HITECH compliance.

1. **Business Owner** - An individual who has ultimate responsibility for an Information Asset.

2. **Controller** - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

3. **Data Breach** - An inappropriate disclosure of Personal Data. Examples include sending Personal Data to the wrong email, sending patient data to the wrong patient, losing hard copies of Personal Data, or losing an unencrypted laptop or device with locally stored Personal Data.

4. **Data Protection Laws** - The Data Protection Act (1998), the General Data Protection Regulations, 2016 (GDPR) and any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument of the UK (or guidance or codes of practice issued by any relevant Supervisory Authority), the e-Privacy Directive and the GDPR once it takes effect (in each case as amended, consolidated, re-enacted or replaced from time to time).

5. **Data Subject** - An identified or identifiable natural person.

6. **Information Asset** - A collection or individual piece of information in any form that is eligible for classification (e.g. sensitive, IP, restricted) by the Company in order to effectively protect, retain, and use as part of official Company business.

7. **Information Asset Owner** – An individual who has responsibility for configuration, maintenance, and support of system, process, application, or paper records in a manner that meets the needs of the Business Owner.

8. **Personal Data** - 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.

9. **Personnel** - All employees of the Company whether in a permanent, temporary or Agency capacity, all secondees (*i.e.* those temporarily transferred) employed by the Company, and all contractors (and their staff), together with any sub-contractors, engaged by the Company to perform services.

10. **Processor** - A natural or legal person, public authority, agency or other body, which Processes Personal Data on behalf of the Controller.

11. **Processing** - Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

12. **Profiling** - Any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

13. **Sensitive Personal Data** - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, and data concerning a person's health or sexual orientation.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Global Privacy Policy – General Data Protection Regulation
PAGE: 4 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: May 25, 2018	**REFERENCE NUMBER:** IP.GEN.005
APPROVED BY: Ethics and Compliance Policy Committee	

14. **Third Parties** - All entities other than those who are part of the Company.

PROCEDURE:

Personnel must consult the DPO at the earliest stage on all issues relating to data protection and involve the DPO in all risk assessments where there is any potential risk to the rights of the Data Subjects.

Data Breach Notification

1. The DPO will notify the relevant Supervisory Authority of Data Breaches within 72 hours of any security, unauthorised access, or distribution of Personal Data unless such breach is unlikely to result in serious harm to the individual including harm to their privacy.
2. If the breach has the potential for serious harm to an individual's rights and freedoms, that individual must be notified without undue delay unless certain exceptions (set out in the Data Protection Laws) apply.
3. To ensure compliance with the requirements (in 1 and 2 above) all Personnel must immediately report any actual, suspected or alleged breach to his/her manager and the DPO by documenting the issue in the designated incident reporting tool. Personnel must provide information and support to any breach investigation as directed by DPO.
4. The Information Governance Manager or designee will document, monitor, investigate and provide incident reports on any actual, suspected or alleged breach, as instructed by the DPO.

Data Subject Rights

1. The Company will, if applicable, provide the Data Subject a copy of their Personal Data without undue delay and at the latest within one month and explain any relevant exemptions which have been applied, where data is not provided.
2. The Company will put appropriate procedures in place to enable Data Subjects to exercise the rights granted by the Data Protection Laws. These include the right to Data Portability, Rectification and Erasure, Right to Restrict Processing and Objection to Processing.

REFERENCES:

1. General Data Protection Regulation (2016)
2. Article 29 Data Protection Working Party Guidelines on Data Protection Officers (2016)
3. International Standard – ISO/IEC 27002:2013 Information Security Management
4. European Union Regulation 2016/679 General Data Protection Regulation
5. United Kingdom Data Protection Act of 1998
6. International Division Information Security Policies
7. Information Protection Patient Privacy Policies, IP.PRI
8. Information Security Common Terminology
9. Information Security Standards
10. Information Security Roles and Responsibilities Policy, IP.SEC.006
11. Information Security Risk Acceptance and Accountability Policy, IP.SEC.009
12. Information Lifecycle Management Policy, EC.014