HCA HEALTHCARE UK POLICY
CORPORATE INFORMATION SECURITY DATA PROTECTION

Document Number: HCAUK.GOV.IS.POL.1008 1.0	Publication Date: 02/07/2018
Review Date: 02/01/2021	Document Owner: Chief Information Officer
Expiry Date: 02/07/2021	Approved by: Executive Director/ VP Legal Services 
Replaces Document: HCAUK.GOV.IS.POL.004	
Target Audience: HCA Healthcare UK and all Company-affiliated facilities, Company business units and all Corporate Departments	Date approved: 02/07/2018
Document Summary:	Outlines measures to ensure patients, colleagues and business partners trust HCA Healthcare UK to handle information about them / their interests in a confidential manner.
Key words:	Confidential, General Data Protection Regulation, GDPR, Data Protection, personal, database, data, exchange.
Key linked policies/ guidelines	Corporate Information Security – Programme Requirements Corporate Information Confidentiality and Security Agreements Policy Corporate Information Security - Roles and Responsibilities Policy Corporate Information Security – Confidentiality Agreements Policy

Version Tracking		Changes made to document
Date	Version Number	
23/05/2018	3.0	Replaces document HCAUK.GOV.IS.POL.004

Contents

1 SCOPE

HCA Healthcare UK and all Company-affiliated facilities, Company business units and all Corporate Departments

The policy applies to information retained in all structured filing systems;

- paper based or electronic (including data on individual PCs),
- other media linked to an individual (e.g. an X-Ray),
- verbal communication by employees and CCTV records.

2 PURPOSE

To comply with current privacy legislation in relation to personal confidential information and that all company confidential information is secure and accurate.

To ensure patients, colleagues and business partners trust HCA Healthcare UK to handle information about them / their interests in a confidential manner.

3 POLICY

1. Confidential data (about HCA Healthcare UK patients, employees and other individuals) and sensitive business information about HCA Healthcare UK must be:
   - obtained, used, shared and transferred,
   - stored and disposed of in a professional, legal and ethical manner, whether at an HCA Healthcare UK site or elsewhere.
2. The requirements of the General Data Protection Regulation (GDPR), Data Protection Act 1998 (DPA98), and other applicable data protection laws must be met:
   - Data confidentiality industry standards and appropriate supporting guidance are advised to assure appropriate organizational and technical controls are selected to protect data; and
   - Security measures and audit procedures must be in place to assure compliance.

4 PROCEDURE

4.1 Core compliance actions

1. Personal information, as defined in the GDPR and Data Protection Act 1998, must be maintained such that it is accurate, appropriately available and used in compliance with DPA98 Principles.
2. The number of databases containing confidential information must be kept to a necessary minimum.
   a) Where systems assign a patient identifier, it must be clear which the master record (Meditech) is. Other databases must use this identifier where possible.
   b) All databases must be kept at secure HCA Healthcare UK owned or controlled premises.

3. Confidential personal data should not be kept on mobile (laptop) computers or mobile communication devices.
    a) In case of inadvertent data storage, all computer and mobile devices / storage media must be encrypted.
    b) Exceptions must be subject to additional protections e.g. to ensure data is not disclosed inappropriately and that master records are kept up to date.
4. Confidential information in physical format (e.g. on paper or USB sticks) should not, as a principle, be removed from secure locations at HCA Healthcare UK premises.
    a) Where off site transfer of databases is essential, great care with passwords, back up and physical security measures must be taken (e.g. encryption techniques) used.
5. Specific procedures supporting the principles of the GDPR, 1998 Data Protection Act (e.g. data sharing and data transfers), and DOH Access to Health Records guidance must be in place (and employees trained in their application) to ensure compliance with legislation.

4.2 Responsibilities

1. Responsibility lies with every individual employee to make sure that confidential information is accurate, properly documented and handled in accordance with this policy.
2. Senior responsibilities:

Data Protection Activity	Responsible Party
Group Data Protection Controller	President & Group CEO
Data Protection Controller/Officer (site)	Chief Executive Officer
Notification on behalf of the company to the ICO or CQC	Executive Director / VP of Legal or DPO
Monitoring compliance	Information Governance Board (IGB) Information Governance and Security Council (IGSC)
Management of specific databases	Business Owner / Head of Department

4.3 Third Party Data

1. HCA Healthcare UK does not, as a general rule, store or take responsibility for data owned by 3rd parties.
    a) This policy must be made clear in any contractual agreements with the 3rd party.
    b) Where a 3rd party requests data management services, HCA Healthcare UK may provide advice on a "without prejudice" basis and shall not accept responsibility for any consequential losses incurred as a result of reliance placed on its advice.
    c) The 3rd party is responsible for compliance with GDPR and DPA98 in relation to their own data and confidential documentation when on HCA Healthcare UK premises.

2. If HCA Healthcare UK does provide a data management services for a 3rd party, contractual arrangements must include commitment by the 3rd party to comply with HCA Healthcare UK IS policies and standards, and to cooperate with all HCA Healthcare UK requests in relation to data protection compliance.
    a) Where a 3rd party (e.g. a consultant) uses a system provided by HCA Healthcare UK (e.g. for practice management), HCA Healthcare UK retains control of the data within the HCA Healthcare UK system.
    b) HCA Healthcare UK policy compliance must be built into contracts. The 3rd party is responsible for compliance with GDPR and DPA98 in their use of their data and documentation.
    c) The Responsible Manager (e.g. at a diagnostic centre offering systems support) must ensure processes are in place to promote and demonstrate GDPR and DPA98 compliance.
3. Where there is a joint venture, HCA Healthcare UK will include a specific agreement covering responsibilities for data management in the contract terms, to ensure compliance with the provisions of the Data Protection Act.

4.4 Information Confidentiality Agreements with Individuals

1. In order to protect HCA Healthcare UK confidential data, all those with access to such material must sign a confidentiality agreement in line with Policy HCAUK.GOV.IS.POL.1009.
    a) Managers responsible provision of access should to include a confidentiality briefing making clear HCA Healthcare UK's expectations in relation to GDPR and DPA98 compliance

4.5 Data Exchange Arrangements

a) 3rd parties involved with data exchange must agree and sign a protocol agreement / contract as part of the initiating negotiations.
    a) The protocol / contract must be adjusted according to specific circumstance by the responsible Manager who maintains the agreement documentation and ensures that the protocol is approved, if site specific, by relevant CEOs.
    b) Protocol / contract text must be approved by a Corporate Director with advice from Legal and IT&S.
        i. GDPR and DPA98 mandates specific clauses and conditions for confidential data being transferred outside the EU
        ii. The NHS access requirements mandate similar precautions for confidential data being transferred outside the UK
    c) An HCA Healthcare UK representative authorized to approve access to HCA Healthcare UK information system and/or the disclosure of the sensitive HCA Healthcare UK information must sign the document(s).

2. Signed agreements must be retained by the Manager owning the third party relationship.
    a) The document(s) must include provisions governing the 3rd party's information security policies & practices and compliance with legislation, regulatory requirements and HCA standards.
    b) Contract provisions must be approved by the Legal Department.
3. Additional contracts, if 3rd party workers are outside the EU, must comply with GDPR and DPA98 legislation. The responsible manager must consult Legal to ensure contract compliance.
4. If clinical information relating to patient treatment is transferred to third parties outside HCA Healthcare UK's normal contract relationships, then action must be taken to ensure compliance with the GDPR and DPA98

5 REFERENCES

1. General Data Protection Regulation (EU) 2016
2. The Data Protection Act 1998 and subsequent directives from the Information Commissioner's Office
3. HCA Healthcare UK Healthcare Code of Conduct
4. Information Security – Programme Requirements HCAUK.GOV.IS.POL.1012
5. Information Confidentiality and Security Agreements Policy, HCAUK.GOV.IS.POL.1009
6. Information Security Roles and Responsibilities Policy, HCAUK.GOV.IS.POL.1010
7. HCA Healthcare UK Healthcare UK Information Security Standards
8. Information Governance Handbook: Section 1 Introduction: Managers IG responsibilities NHS N3 Access Accreditation Requirements
9. Information Governance Handbook: Section 2 for guidance on many aspects of electronic communications designed to assist users to comply with this policy
10. Information Governance Handbook: Section 4 Access Management Electronic Communications Guidance for Managers CQC and NHS network access accreditation requirements.
11. Health and Social Care Act 2008, Requirement 24
12. The Information Commissioner's Office web site: http://www.ico.gov.uk/
13. NHS Connecting for Health web site Access to Health Records, Department of Health Guidance 2010: http://www.connectingforhealth.nhs.uk/

- End Document -