



LOTUS HEALTHCARE

5 Devonshire Place, Marylebone, London W1G 6HL
Tel: 020 3474 0800 - Email: info@lotushealthcare.co.uk

Care Quality Commission (CQC) FUNDAMENTAL STANDARDS

Policy title:	Confidentiality and data protection.
Regulation:	17 (2) (c) (d) - Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
Outcome:	All records relating to peoples' health, staff employment records, and organisation records are stored securely and confidentially in line with current legislation.
Authorised by:	Dr Mayank R. Shah, MBBS DRCOG DFSRH Medical Director (CQC Registered Manager)
Issue date:	1 March 2018
Review date:	28 February 2019 (or before if there is a change in practice or circumstances)

1. Policy statement

- 1.1 The Lotus Healthcare independent healthcare service is fully committed to complying with the Data Protection Act 1998 which came into force on 1 March 2000.
- 1.2 It is important that Lotus Healthcare protects and safeguards patient-identifiable (or person-identifiable) and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law, and to provide assurance to patients who use the healthcare services on offer.
- 1.3 All employees of Lotus Healthcare are bound by a legal duty of confidentiality to protect personal information they may come into contact with during the course of their work.
- 1.4 This policy sets out the principles that must be observed by all staff who work within Lotus Healthcare and have access to person-identifiable information or confidential information.
- 1.5 All members of staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.
- 1.6 Respect for confidentiality is an essential requirement for Lotus Healthcare as an independent healthcare provider.

2. Data protection

- 2.1 The ease with which personal information can be passed within Lotus Healthcare - often electronically - is a benefit for patients and for those involved in their care and treatment. However, all staff need to be aware of their legal responsibilities under the Data Protection Act to protect the confidentiality of patient information, and other information relating to the business activities of Lotus Healthcare.
- 2.2 Personal information on staff is also protected by the Data Protection Act. The Act affords members of staff the same rights of protection for, and of access to, their personal information held by Lotus Healthcare.
- 2.3 The term '**person-identifiable information**' refers to information relating to any identifiable individual and it is important to be aware that healthcare information is considered in the Data Protection Act to be 'sensitive information' requiring the highest levels of care and protection.
- 2.4 Lotus Healthcare fully supports and complies with the principles of the Data Protection Act. In summary, this means personal information must be:
- processed fairly and lawfully
 - processed for limited purposes and in an appropriate way
 - adequate, relevant and sufficient for the purpose
 - accurate and up-to-date
 - kept for as long as is necessary and no longer
 - processed in line with individuals' rights
 - secure and protected against unlawful access, loss or damage, and
 - only transferred to others that have suitable data protection controls.
- 2.5 Everyone working for Lotus Healthcare who records, handles, stores or otherwise comes across information, has a statutory duty under the Data Protection Act, along with a duty of confidentiality in common law, to patients and to Lotus Healthcare as an employer.

These duties apply equally to staff who are permanent or temporary, full or part-time, agency or bank staff, staff who have been granted practising privileges, students or trainees, volunteers, or to staff on temporary placements.

- 2.6 Lotus Healthcare will follow procedures to ensure that all employees, contractors, agents, consultants and other relevant parties who have access to any personal information held by, or on behalf of Lotus Healthcare, are fully aware of and abide by their duties and responsibilities under the Act.

3. Roles and responsibilities

3.1 The Medical Director

The Medical Director has overall responsibility for maintaining confidentiality within Lotus Healthcare and ensuring that this policy is complied with by all staff.

3.2 All members of staff

All staff have a responsibility to protect the personal information held by Lotus Healthcare.

Each member of staff will be expected to take steps to ensure that personal data is kept secure at all times and protected against unauthorised, unlawful or accidental loss, damage or disclosure. This applies to all personal identifiable information held in all formats, whether is it in patients' healthcare records or staff employee files, or in any other format such as diaries, message books, notebooks, appointment books, emails and other notes held about individuals.

In particular staff must ensure that:

- they are appropriately trained and knowledgeable in the handling of personal information
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- where they are required to take personal information away from the Lotus Healthcare clinic premises as part of their work, including information held in all formats, this should be held securely at all times and everything possible done to safeguard against unauthorised access or accidental loss or damage
- personal information is transferred securely at all times, whether it is being sent electronically or by surface post
- personal data held on computers and computer systems is protected by the use of secure passwords, and
- all relevant policies are adhered to when processing personal data to ensure adequate levels of protection are maintained.

Where staff, as part of their Lotus Healthcare responsibilities, collect, hold and process information about other people, they must comply with this policy. No-one should disclose personal information outside this policy or use personal data held about others for their own purposes.

All healthcare professionals practising within Lotus Healthcare have professional and ethical duties of confidentiality within their respective codes of conduct which they are expected to follow.

4. Person identifiable information

- 4.1 Person-identifiable information is anything that contains the means to identify a person, e.g. an individual name, address, postcode, date of birth, email address, telephone number, or unique identifiable reference number.
- 4.2 Confidential information within Lotus Healthcare is not restricted to a person's health information. It also includes private information that an individual would not expect to be shared such as staff employee records, occupational health records, and business information about Lotus Healthcare.
- 4.3 Information can relate to Lotus Healthcare patients and staff (including temporary staff), however stored. Information may be held in:
- paper format
 - computers
 - laptops
 - tablet devices
 - mobile phones
 - digital cameras
 - compact discs (CDs)
 - digital versatile discs (DVDs), and
 - USB devices.

This list is not exhaustive.

5. Disclosure of personal information

- 5.1 Strict conditions apply to the disclosure of personal information within Lotus Healthcare. Lotus Healthcare will not disclose personal information to any third party unless it is believed to be lawful to do so.
- 5.2 Information relating to identifiable patients must not be divulged to anyone other than an authorised person, for example medical, nursing or other healthcare professional staff, as appropriate, who are concerned directly with the care, diagnosis and/or treatment of the patient.
- 5.3 Maintaining confidentiality is an important duty but there are circumstances when it may be appropriate to disclose confidential patient information. These are:
- when the patient has given consent
 - when the law says it must be disclosed, or

- when it is in the public interest to do so.

An example of such circumstances would be child protection where the overriding principle is to secure the best interests of the child.

5.4 Lotus Healthcare will also seek the consent of staff for the passing on of identifiable personal information for any purpose other than those outlined to staff on appointment. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- Lotus Healthcare has the statutory power or is required by law to do so, or
- the information is clearly not intrusive in nature, or
- the member of staff has consented to the disclosure, or
- the information is in a form that does not identify individual employees.

5.5 If staff have any concerns about disclosing information they must discuss this with Medical Director.

6. Caldicott principles

6.1 The following seven Caldicott principles will be adhered to by Lotus Healthcare in all cases where the appropriate use of person identifiable health information is considered.

Principle 1

Justify the purpose

Every proposed use or transfer of personal confidential data within or from, Lotus Healthcare should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by the Medical Director.

Principle 2

Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be used unless it is essential for the specified purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose.

Principle 3

Use the minimum necessary personal confidential data Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

Principle 4

Access to personal confidential data should be on a strict need to know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see.

Principle 5

Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6

Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements. In Lotus Healthcare, this is the Medical Director.

Principle 7

The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of patients within the framework set out by these principles. They should be supported by policies of their respective regulators and professional bodies.

Examples of justifiable purposes include:

- delivering personal care and treatment
- assuring and improving the quality of care and treatment
- monitoring and protecting public health
- managing and planning healthcare services
- risk management
- investigating complaints and potential legal claims
- teaching purposes
- statistical analysis, and
- medical or health services research.

The above principles do not and cannot provide definitive answers for every situation as much depends on the context of each individual case. If in doubt, staff working at Lotus Healthcare must seek appropriate advice from the Medical Director before releasing personally identifiable information.

7. Handling of personal information

- 7.1 Lotus Healthcare will handle all person-identifiable information securely and in keeping with the requirements of the Data Protection Act.

- 7.2 All staff, through appropriate training and responsible management, will be expected to:
- fully observe conditions regarding the collection and use of personal information
 - meet legal obligations to specify the purposes for which personal information is gathered and used
 - collect and process appropriate personal information only to the extent that it is needed to fulfil Lotus Healthcare's operational needs or to comply with any legal requirements
 - apply strict checks to determine the length of time personal information is held, and
 - take appropriate technical and organisational security measures to safeguard personal information.
- 7.3 Lotus Healthcare will take disciplinary action against any member of staff found to have breached patient confidentiality, and ensure that all staff are aware that they risk personal prosecution for breaches of the Data Protection Act.

8. Compliance

- 8.1 Lotus Healthcare will ensure that:
- there is always someone with specific responsibility for Data Protection in Lotus Healthcare
 - patients are pro-actively informed of the uses to which their information is put
 - staff are informed, on appointment, of the uses to which their personal information is put, e.g. equal opportunity monitoring
 - consent is sought before passing personal identifiable information on for any reason other than to fulfil justifiable purposes
 - staff are reminded of their obligations under the Data Protection Act
 - everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice
 - only staff who need access to personal information as part of their duties are authorised to do so. Unauthorised access to personal information, either in paper or electronic format, is considered to be a breach of the Data Protection Act and this Lotus Healthcare policy

- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised, where necessary
- anyone wishing to make enquiries about handling personal information knows what to do
- queries about handling personal information are dealt with promptly and courteously
- methods of handling personal information are clearly described, and
- the way personal information is managed and handled will be regularly reviewed and evaluated.

9. Breaches of confidentiality

9.1 Breaches of confidentiality are often unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences could be equally serious for all concerned.

9.2 Obligations to maintaining confidentiality and preventing breaches include;

- not gossiping
- taking care not to be overheard when discussing a patient's circumstances in a public area
- closing and locking doors/cabinets/drawers when not in use
- not leaving a computer unattended and logged-in
- always logging out of a computer when work is finished or when leaving a desk
- making sure computer screens are never visible to the public, especially in public reception areas
- querying the status of visitors and strangers to Lotus Healthcare, and
- knowing who to tell if anything is suspicious or worrying.

9.3 The simple rule of thumb is that personally identifiable information must always be held securely and, when used, treated with respect.

This rule applies whether the information is held in paper format, in a computer, or in a member of staff's head.

10. Policy awareness

- 10.1 All new members of staff at Lotus Healthcare will be made aware of this policy through their induction programme.
- 10.2 Existing staff will be reminded of the policy which will be readily accessible within Lotus Healthcare.
- 10.3 All staff and relevant third parties must be familiar with and comply with this policy at all times.

11. Guidance and further reading

- Caldicott Guardian Manual 2006 (DH, 2006)
- Care Quality Commission (Registration) Regulations 2009
<http://www.legislation.gov.uk/uksi/2009/3112/contents/made>
- Care Quality Commission (Registration) and (Additional Functions) and Health and Social Care Act 2008 (Regulated Activities) (Amendment) Regulations 2012 (Amendment to Parts 4 & 5)
<http://www.legislation.gov.uk/uksi/2012/921/contents/made>
- Care Quality Commission (Registration and Membership) (Amendment) Regulations 2012
<http://www.legislation.gov.uk/uksi/2012/1186/contents/made>
- Confidentiality: NHS code of practice (DH, 2003)
- Data Protection Act 1998
<http://www.legislation.gov.uk/ukpga/1998/29/contents>
- Employment Rights Act 1996
<http://www.legislation.gov.uk/ukpga/1996/18/contents>
- Equality Act 2010
<http://www.legislation.gov.uk/ukpga/2010/15/contents>
- Freedom of Information Act 2000
<http://www.legislation.gov.uk/ukpga/2000/36/contents>
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
<http://www.legislation.gov.uk/uksi/2014/2936/contents/made>
- The Health and Social Care Act 2008 (Regulated Activities)(Amendment) Regulations 2015
<http://www.legislation.gov.uk/uksi/2015/64/regulation/14/made>
- Health Professional Council – legal framework
<http://www.hpc-uk.org/aboutus/legislation/>

- Health and Safety at Work etc. Act 1974
<http://www.legislation.gov.uk/ukpga/1974/37/contents>
- Information security management: NHS code of practice (DH, 2007)
- Mental Capacity Act 2005 and associated code of practice
<http://www.legislation.gov.uk/ukpga/2005/9/contents>
<https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice>
- Mental Health Act 1983
<http://www.legislation.gov.uk/ukpga/1983/20/contents>
- Mental Health Act 2007
<http://www.legislation.gov.uk/ukpga/2007/12/contents>
- NHS Information Governance: Guidance on Legal and Professional Obligations (DH, 2007)
- Records management: NHS code of practice (DH, 2006),
- Relevant professional guidance and codes of conduct and practice relating to record keeping published by professional bodies and registration councils including the General Medical Council, Nursing & Midwifery Council, General Social Care Council, BMA, RCN, Health and Care Professions Council, Royal College of Physicians and the Academy of Medical Royal Colleges
- Safeguarding Vulnerable Groups Act 2006
<http://www.legislation.gov.uk/ukpga/2006/47/contents>

Signature **Date**

**Dr Mayank R. Shah, MBBS DRCOG DFRH
Medical Director (CQC Registered Manager), Lotus Healthcare Limited**