Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

Confidentiality and Data Protection Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	08.02.2024	Carolina Guariniello – Operations Manager	Paul Flynn – CQC Registered Manager	Formatted to fit in the new the Policies template.

1 Policy statement

The Addcounsel independent healthcare service is fully committed to complying with the Data Protection Act 1998 which came into force on 1 March 2000 and the General Data Protections Regulation (GDPR) that came in to force on 25th May 2018.

It is important that Addcounsel 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.

All employees of Addcounsel are bound by a legal duty of confidentiality to protect personal information they may come into contact with during the course of their work.

This policy sets out the principles that must be observed by all staff who work within Addcounsel and have access to person-identifiable information or confidential information.

All members of staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

Respect for confidentiality is an essential requirement for Addcounsel as an independent healthcare provider.

2 General principles

2.1 Data protection

The ease with which personal information can be passed within Addcounsel - 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 and GDPR to protect the confidentiality of patient information, and other information relating to the business activities of Addcounsel.

Personal information on staff is also protected by the Data Protection Act. And GDPR legislation. The Act affords members of staff the same rights of protection for, and of access to, their personal information held by Addcounsel.

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.

Addcounsel fully supports and complies with the principles of the Data Protection Act and GDPR legislation. 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.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

- secure and protected against unlawful access, loss or damage, and

- only transferred to others that have suitable data protection controls.

Everyone working for Addcounsel 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 Addcounsel 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.

Addcounsel 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 Addcounsel, are fully aware of and abide by their duties and responsibilities under the Act.

2.2 Person identifiable information

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.

Confidential information within Addcounsel 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 Addcounsel.

The data that falls under the General Data Protections Regulation is

- Name
- Photo
- Email address.
- Social media posts
- Personal medical information
- IP addresses
- Bank details.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

Information can relate to Addcounsel 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.

2.3 Disclosure of personal information

Strict conditions apply to the disclosure of personal information within Addcounsel. Addcounsel will not disclose personal information to any third party unless it is believed to be lawful to do so.

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.

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

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

- 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.

Addcounsel 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:

- Addcounsel 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.

If staff have any concerns about disclosing information, they must discuss this with the Operations Manager.

2.4 Caldicott principles

The following seven Caldicott principles will be adhered to by Addcounsel 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, Addcounsel should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by the Operations Manager.

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.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

Principle 3
Use the minimum necessary personal confidential data Where use of personal confidential data is 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 Addcounsel, this is the Operations Manager.

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

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

- 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 Addcounsel must seek appropriate advice from the Operations Manager before releasing personally identifiable information.

2.5 Handling of personal information

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

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 Addcounsel'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.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

Addcounsel 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.

2.6 Compliance

Addcounsel will ensure that:

- there is always someone with specific responsibility for Data Protection in Addcounsel
- 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 Addcounsel policy.
- everyone managing and handling personal information is appropriately trained to do so.
- everyone managing and handling personal information is appropriately supervised, where necessary

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

- 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.

2.7 Breaches of confidentiality

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.

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.
- making sure computer screens are never visible to the public.
- querying the status of visitors to Addcounsel, and
- knowing who to tell if anything is suspicious or worrying.

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

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

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

2.8 Policy awareness

All new members of staff at Addcounsel will be made aware of this policy through their induction programme.

Existing staff will be reminded of the policy which will be readily accessible within Addcounsel.

All staff and relevant third parties must be familiar with and always comply with this policy.

3 Responsibilities

Operations Manager
The Operations Manager has overall responsibility for maintaining confidentiality within Addcounsel and ensuring that this policy is complied with by all staff.

All members of staff
All staff have a responsibility to protect the personal information held by Addcounsel.

Each member of staff will be expected to take steps to ensure that personal data is always kept secure 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.

Staff must ensure that:

- they are appropriately trained and knowledgeable in the handling of personal information.

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

- 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 an Addcounsel healthcare environment 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 always transferred securely, whether it is being sent electronically or by surface post.

- personal data held on computers and computer systems is protected using 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 Addcounsel 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 Addcounsel have professional and ethical duties of confidentiality within their respective codes of conduct which they are expected to follow.

4 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)

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

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
- General Data Protection Regulation 2018

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

- 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

addcounsel

Universal House
1 Merus Court
Meridian Business Park
LE19 1RJ

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:	DocuSigned by: paul flynn DC450BA452B445E...
Date:	16/2/2024 | 1:23 AM PST
Name and role:	Paul Flynn – CEO and CQC Registered Manager