Privacy and Confidentiality Policy

Generated in line with NHS England guidelines

Introduction

- The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Conatus and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.
- All employees working in the Conatus are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the General Data Protection Regulations 2018.
- It is important that Conatus protects and safeguards person identifiable and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law, relevant advisory bodies mandatory requirements and to provide assurance to patients and the public.
- This policy sets out the requirements placed on all staff when sharing information within and outside of the organisation.
- Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted.
- Confidential information within Conatus is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including employee records, occupational health records, etc. It also includes Conatus confidential business information.
- Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Clinical Director. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager.

The following list gives examples of breaches of this policy which should be reported:

- Sharing of individualised passwords
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the General Data Protection Regs.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.

- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing of person identifiable information in ordinary waste paper bin.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Confidentiality Dos and Don'ts

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is an obligation on everyone working or on behalf of Conatus.
- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely when necessary i.e. use the appropriate account to send confidential information to another.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Please report any actual or suspected breaches of confidentiality to:

Dr Alastair Barnett on 01926 678085.