Alamac Confidentiality and Privacy Policy (GDPR)
April 2018
Review March 2019

INTRODUCTION

This policy sets out Alamacs approach to the General Data Protection Regulation 2018 (GDPR) and applies to all personal data held by Alamac relating to any identifiable living person. Personal information held about our clients will be handled sensitively and confidentially by all employees, Associates and Members of our Board.

It should be noted that sensitive information relates to past, present and future clients with whom we have dealings, including data held on past, present and future staff.

POLICY STATEMENT

All employees, Associates and Board Members **must** comply with this policy. All employees need to be aware of their responsibilities under GPPR for safeguarding confidentiality and preserving information security in respect of commercially sensitive data. Alamac expects that no employee shall misuse any confidential information or allow others to do. Alamac expects that employees:

- Treat all personal and sensitive information as confidential
- Comply with the law regarding the protection and disclosure of information
- Not disclose information without the prior informed consent of the individual concerned, (except in the circumstances where otherwise permitted by the law)
- Not attempt to gain access to information they are not authorised to have
- All personal information about Alamac clients and its subsidiaries will be:

    - Obtained, held and processed fairly
    - Held for specific purposes and used only for those purposes
    - Relevant, accurate and kept up to date
    - Corrected if shown to be inaccurate
    - Kept no longer than is necessary and destroyed when no longer required, in line with best practice
    - On request, made available to the data subject

POLICY OBJECTIVES

- To ensure compliance with the GDPR and regulatory requirements in relating to confidentiality
- To ensure all Alamac employees are aware of, and understand the importance of, data protection and confidentiality
- To ensure the protection of personal and sensitive information of clients and employees
- To ensure clients are able to have access to their own information within relevant timescales
- To ensure procedures are in place across Alamac employees, Associates and Board Members regarding disclosure of personal information
- To ensure all Alamac employees, Associates and Board Members receive appropriate data protection training, with regular updates or when significant data protection guidance changes

CALDICOTT

Although employees of Alamac do not collect or record any patient information, nor do any of our databases or systems hold any patient information, some staff may be exposed to patient information when working within the clinical environment. As such we have adopted the Caldicott principles:

In 1997 the Chief Medical Officer commissioned a review to investigate the ways in which patient information was used in the NHS. The findings were published in The Caldicott Report and made a number of recommendations aimed at improving the way the NHS handles information.
Originally 6 Caldicott Principles were identified which provide a framework of good practice which should be adopted by all staff who have access to patient information. The paper has now been reviewed and a seventh principle has been added; the duty to share information can be as important as the duty to protect patient confidentiality.

1) **Justify the purpose(s).** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2) **Don't use personal confidential data unless it is absolutely necessary.** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
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 is transferred or accessible as is necessary for a given function to be carried out.
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. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
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.

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.

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 their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

RESPONSIBILITIES AND REQUIREMENTS

All employees have a responsibility to effectively manage personal data. The Chief Operating Officer (COO) is responsible for ensuring all employees, Associates and Board Members receive adequate training.

Any person may ask Alamac for the data that they hold about them. Any such request should be immediately passed to the COO for action (a response must be made within 30 calendar days)

Any data that the person is entitled to see must be presented in plain language in hard copy format. Additionally, where necessary, the information will be provided verbally.

From 25 May 2018 subject access requests (SAR) are provided free of charge

ACCESS TO INFORMATION AND DISCLOSURE OUTSIDE ALAMAC

Alamac employees will generally have access to all the information they need to carry out their work and uphold their duty to keep that information confidential. In the unlikely event that any information needs to be disclosed to someone outside Alamac, the employee or Associate must explain to an individual why this is necessary and obtain written consent before doing so. If an individual does not give consent, this should be noted and special arrangements should be made for recording information and access to it.

There are certain situations where, by law, employees and Associates do not have to obtain prior permission to disclose personal information about individuals. These are:

To comply with the law (e.g. the police, Inland Revenue, Council Tax Registration Office or a court order).

- Where there is a health and safety risk
- When there is evidence of fraud
- Anonymously for bona fide statistical reporting or research purposes, providing it is not possible to identify the individual to whom the information relates
- Where specifically enabled by the terms of registration of the GDPR
- Where there are declarations of interest by employees, Associates or Board members

Care must be taken to ensure that enquirers have a legitimate right to have access to the information that they ask for, so that information is only shared on a "need to know" basis. Always be mindful that people may try to obtain information by deception. ****NOTE:** Requests for access to health records must be referred to the Chief Operating Officer.

ANONYMISATION AND PSEUDONYMISATION

Organisation/Person-identifiable information should be omitted where anonymised information is sufficient. Do not use organisation/patient-identifiable information unless it is essential for the purpose. All disclosure of anonymised information should be reviewed on a case by case basis. Pseudonymised information is subject to the same strictures as anonymised information.

ABUSE OF PRIVILEGE

All Alamac employees are forbidden to access any personal information relating to colleagues, friends, relatives, or any other person unless they have legitimate reason to do so as part of their employment responsibilities.

STORAGE OF CONFIDENTIAL INFORMATION

Confidential and sensitive information should be held on the network server and data must be regularly backed up. Employees must lock their PC using **Ctrl-Alt-Delete** when left unattended to maintain security of electronic records.

CONFIDENTIALITY OF PASSWORDS

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone. Passwords should not be written down.

PASSWORD SECURITY

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the Chief Operating Officer.

SOCIAL MEDIA

Social media is defined as interactive online technology tools that allow individuals to exchange and share information and resources, including pictures, instantly via the internet. This includes online blogs, personal websites, discussion boards, email groups, instant messaging and also forums such as Facebook, Twitter and LinkedIn. This list is not intended to be exhaustive as this is a constantly evolving area. Employees should follow Alamac Social Media policy in relation to any social media that they use.

If a member of staff identifies an association with Alamac or any of our partners/clients, discusses their work and/or colleagues, or comes into contact, or is likely to, with service users on any social media sites, they will behave appropriately and in a way which is consistent with Alamacs values, how they would wish to present themselves with colleagues, patients and service users and where relevant in line with their professional code of conduct.

Employees who may not directly identify themselves as an Alamac employee when using social media for personal purposes should be aware that content they post on social media websites could still be construed as relevant to their employment with Alamac. For example employees should not take photos on site or upload them, write or report on conversations, meetings or matters that are meant to be private or internal, or disclose confidential information. Employees should not cite or make reference to clients, service users, partners or providers without their written approval.

COMMERCIALLY SENSITIVE INFORMATION

Any form of information that could adversely prejudice the commercial interests/activities of Alamac or any of our clients, or individual should be considered as confidential and be used or disclosed to third parties unless required by exception.

BREACHES OF THIS POLICY AND INVESTIGATION OF INCIDENTS

A breach of confidentiality is defined as any action or incident which has been caused, or could result in, the wilful or accidental unauthorised access, disclosure, alteration, corruption or deletion of any data held on or produced by a computer which relates to a client, a member of staff or the commercial activities of Alamac and its purchasers and suppliers. Examples of breaches in confidentiality include:

- Deliberately looking at records without authority
- Discussion of personal details in inappropriate venues
- The disclosure or loss of confidential information
- Unauthorised use of information
- Unsecure or unauthorised disclosure of person identifiable information to a third party

** **NOTE:** This list is not exhaustive and applies to all paper and electronic records.

The incident should be reported to the Chief Operating Office as soon as is possible, and will be investigated by the Chief Operating Officer or equivalent deputy who will keep Alamac personnel appropriately informed.

If the breach involves a client the investigation outcomes will be discussed with the client. Lessons learned will be communicated to Alamac employees and any updates and/or amends to the confidentiality policy will be made and all staff informed of the updates. Sanctions for a breach can include disciplinary action, ending a contract, dismissal, or bringing criminal charges.

All employees are individually responsible for reporting security incidents. For further information on reporting incidents see Alamac Incident Policy.

TRAINING

It is the responsibility of the Chief Operating Officer to ensure users are informed of this policy at induction and to inform of any updates and changes to the policy.

INTERPRETATION

If any employee requires an explanation concerning the interpretation or the relevance of this policy, they should discuss the matter with the Chief Operating Officer or the Chair. All relevant policies, procedures and guidance are posted on the Alamac shared drive to which all employees have access.

INFORMATION

Further information on the GDPR can be found here:

www.ico.org.uk