Gaddum

Information Governance Framework Policy

Policy name:	Information Governance Framework Policy
Document created:	February 2016
Document last reviewed:	March 2020
Version no:	4
Review Period:	6 months
Review Date:	September 2020
Approved by:	SMT

Contents:

1. Purpose of the Information Governance Framework

This framework sets out the procedures, responsibilities, accountability and sanctions that have been put in place within Gaddum to safeguard the movement of personal data.

- **Underpinning Procedures**

  The following procedures included in this framework have been put in place to support the confidential handling of information within Gaddum and the sharing of this information with other organisations:

  - **Confidentiality code of conduct** (contains clear guidelines on the disclosure of personal information)
  - **Safe Transfer of Personal Data Policy** (guidelines for sharing data in a lawful manner)
  - **Incident Management Procedure** (sets out the procedures for responding to a security breach)
  - **Business Continuity Plans** (setting out procedures for each site in the event of system failure)
  - **Data Protection Policy** (contains clear guidelines on protecting the rights and privacy of individuals)
  - **Access Control Procedure** (guidelines to restrict access to personal information)
  - **Handling Security Incidents Procedure** (outlining the responsibilities of staff and volunteers if a security incident occurs)
  - **Record Management Policy** (contains guidelines for staff on how to best manage our records)

- **Roles and Responsibilities**

  Board

  The ultimate responsibility for information governance rests with the Board of Trustees, who ensures there are adequate controls in place at Gaddum

  SMT

  Responsible for the day-to-day operation of the charity and ensuring that staff, systems and sub-contractors comply with the requirements of information governance, and reviews all serious incidents involving actual or potential loss of data or breach of confidentiality.

  Information Governance Lead

  Provides advice and guidance to managers and staff on information governance; carries out annual audits reviewing compliance; ensures the framework and policies are updated in line with best practice and learning; ensures staff receiving regular training and updates and participates in the investigation and reporting of information incidents.

Caldicott Guardian

The Caldicott principles have been developed to protect the confidentiality of client information. They are applicable to all identifiable and sensitive client information. The principles are:

- Justify the purpose(s) for using confidential client information
- Only use the confidential information when absolutely necessary
- Only use the minimum confidential information that is required
- Access should be restricted on a need to know basis
- Everyone should be aware of and understand their responsibilities
- Use and handling of personal identifiable information should comply with the law.

The Caldicott Guardian within the Gaddum is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing. The guardian is the Chief Executive at Gaddum.

Managers

Managers are responsible for ensuring that their staff understand and comply with their data access levels and information governance policies and procedures. They ensure the asset register has an up to date record of which staff are allocated equipment. The approve staff access levels and ensure the compliance of all policies and procedures within the framework.

Staff

All employees, whether permanent, temporary, contracted, volunteers or third parties are required to sign an Information Governance agreement confirming that they have read and understood the contents of the policies and procedures, and should remain aware of their responsibility and duty to the compliance of these procedures. This includes maintaining confidentiality of information but also being aware of when it is necessary to disclose confidential information, ensuring secure storage of data and being aware of situations where disclosure may be or may not be required.

Sub-Contractors and Third Parties

They are required to comply with this framework, associated policies and business-level operational procedures and to report any incidents as required. This forms part of the initial due diligence and service level agreement.

- **Accountability and Responsibility for this Policy**

The designated Information Governance Lead in Gaddum is responsible for overseeing the day to day Information Governance issues; developing and maintaining policies, standards and guidance, coordinating Information Governance in Gaddum, raising awareness of Information Governance and ensuring there is ongoing compliance with the policy and its supporting standards and guidelines. This policy has been approved by senior management and will be reviewed on an annual basis or when there are changes in legislation relating to Information Governance.

- **Sanctions**

  Breach of this policy could lead to disciplinary action. Following an investigation, it could lead to dismissal depending on the circumstances.

2. Staff Confidentiality Code of Conduct

Everyone working for Gaddum is under a legal duty to keep service users' personal information confidential (where a serious risk has not been identified). Service users who believe their confidence has been breached may make a complaint to Gaddum and they could take legal action.

This Staff Confidentiality Code of Conduct has been produced to ensure all staff members at Gaddum are aware of their legal duty to maintain confidentiality, to inform them of the processes in place to protect personal information, and to provide guidance on disclosure obligations.

2.1 Scope

The code is concerned with protecting personal information about service users, although its content would apply equally to staff and volunteer personal information. Personal information is data in any form (paper, electronic, tape, verbal, etc.) from which a living individual could be identified; including name, age, address, and personal circumstances, as well as sensitive personal information like race, health, sexuality, etc.

Under the General Data Protection Regulations, the scope also covers genetic, mental, economic, cultural or social identity. Although the General Data Protection Regulation applies to the personal information of living individuals, this code also covers information about deceased service users. The code applies to all staff including permanent, temporary, and locum members of staff.

2.2 Recognise Your Obligations

A duty of confidence arises out of the common law duty of confidence, employment contracts, and for healthcare professionals, it is part of your professional obligations. The **duty of confidence** that all Gaddum staff have is to respect the **confidentiality** of their clients'. Information obtained about their clients' cases may be confidential, and must not be used for the benefit of persons not authorized by the client.

Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution. So, make sure you do not:

- Put personal information at risk of unauthorised access[1];
- Knowingly misuse any personal information or allow others to do so;
- Access records or information that you have no legitimate reason to look at this includes records and information about your family, friends, neighbours and acquaintances.

2.3 Keep Personal Information Private

Make sure you comply with the following staff guidelines which set out practical things you should do to keep personal information protected:

- Good record keeping
- Appropriate use of computer systems
- Secure use of personal information
- Reporting information incidents
- Using mobile computing devices

2.4 Disclose with Appropriate Care

Gaddum will ensure that service users are adequately informed about the use and disclosure of their personal information in a ‘Data Statement’ outlining why, how and for what purpose personal information is collected, recorded and used. The details of this will be available on all of Gaddum sites.

It is each staff member’s responsibility to ensure that their service users’ are aware of where they can access this information, and/or that they are provided with an appropriate copy should they be unable to access it online. You should also ensure that you are familiar with the information and seek advice from the Information Governance lead if service users have questions you are unable to answer.

If you are authorised to disclose personal information you should ensure you do so in accordance with the **information governance procedures** and you must only:

[1] Keeping personal data on a USB or Desktop where theft would render it at risk of unauthorised access; Leaving your desktop/laptop/other device unlocked when you are away from it; emailing identifiable information without first encrypting it within a file; keeping paper copies of client data outside of their correct storage area for longer than is necessary, increasing the risk of loss or unauthorised access

- Share with those with a legitimate right to see/hear the information[2];
- Transfer in accordance with the centre's Safe Transfer of Personal Data Policy;
- Where possible, disclose the minimum necessary to provide safe care;
- Break confidentiality laws if you feel the service user is at serious risk to themselves or others.

If you are authorised to disclose information that can identify an individual service user for non-healthcare purposes (e.g. research, financial audit) you must only do so if:

- You have the service users explicit consent; consent given explicitly by the individual, not on their behalf and with their full understanding of what they are consenting to, in order to ensure there is no later dispute about whether consent was given.

Under the common law duty of confidence, identifiable personal information may be disclosed without consent in certain circumstances, these are:

- Where there is a legal justification for doing so, e.g. to comply with a statute;
- Where there is a public interest justification - i.e. where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

You must refer all requests for disclosure of personal information without the consent of the service user except if you believe them to be a serious risk to themselves or others, including requests from the police, to Gaddum information governance lead.

3. Safe Transfer of Personal Data

Gaddum collects information about potential clients and employees as well as those who use services and who we employ. This information is not the property of Gaddum; it belongs to the people that it has been collected from. Gaddum is merely the custodian, and as custodians we are responsible for the safe keeping and security of all information that comes into our keeping.

[2] As part of a Subject Access Request of the service user themselves have asked to access the information we hold, or the legal parent/guardian who has the right to the information if the service user is a child under the age of 16 and who doesn't appear to have capacity to give consent.

As a data controller[3] or processor[4] of user information you are responsible for ensuring that you handle client information with care and respect. It is your responsibility to protect this information from those who are not authorised to use or view it. You must ensure that whilst in your care you have done everything possible to protect this information.

3.1 Requirements for a Secure Location of Confidential Information

- It should be in an area that is lockable.
- The area should be sited in such a way that only authorised staff can enter that location.
- If the area is on the ground floor, any windows should have locks on them.
- The area should conform to health and safety requirements.
- Manual paper records containing personal information should be stored in locked cabinets when not in use.
- Computers should not be left on view or accessible to unauthorised staff
- Computers should be locked when a staff member leaves their desk and to be switched off when they leave the site.

3.2 Communication by Post

Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked ‘Private and Confidential – to be opened by recipient only.’

The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

If an organisation has a policy that all mail is to be opened at a central point, this policy must be made clear to all partners. An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.

The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

3.3 Communication by Email

The sharing of information within the confines of Gaddum (gaddum.co.uk to gaddum.co.uk email address) does not leave our network and is deemed as

[3] A data controller is the person/persons responsible for collecting data either with clients at sessions or over the phone as well as responsible for deciding what data is collected, what format that is collected in, where it is stored, how it is processed and Data Processors.

[4] A data processor is the person/persons responsible for anyone using viewing, updating or using the data etc.)

secure. However, unnecessarily large amounts of personal data being transferred within this structure should be avoided as best practice.

The transfer of client personal information by email to a third party (outside of the Gaddum network) is not permitted, unless the information has been encrypted. Microsoft Office products such as Word and Excel have the ability to lock documents with a password. The password to unlock the encrypted document should be sent in a separate email to the recipient.

Where a PDF contains personal information and needs to be emailed, we should attempt to covert the file into a Word document to allow for the information to be password protected.

If you are emailing a client, you should take precautions to include little information regarding the service they are receiving, and include only what identifiable information may be necessary (such as first name).

Some services have access to secure systems (such as Egress) in order to share client personal information with third parties. Where these are available, they should be used.

Information should only be shared with the consent of the individual. Gaddum understands that there may be times when information is required for safeguarding purposes and although we should make every effort to ensure that information is still protected within these instances, the client’s welfare takes priority over their data protection.

If there is a data breach, even in the instance of safeguarding purposes, a review will take place to ensure that procedure has been followed and all possible precautions taken to protect data. If you are found to have not taken the appropriate action to protect the data being transferred, you may face disciplinary procedures which could end in dismissal.

3.4 Verbal Communication

A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions.

If information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual/organisation and then calling the recipient back.

Where information is transferred by phone, face to face, care should be taken to ensure that personal details are not overheard by other staff who do not have a ‘need to know.’ Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.

Messages containing personal information should not be left on answer machines unless a password is required to access them. They should also not be stored on communal systems.

Messages containing confidential/sensitive information should not be written on white boards/notice boards.

4. Incident Management Procedures

Ensuring personal information remains confidential and secure is everyone’s responsibility and therefore, it is important that when incidents do occur, the damage from them is minimised and lessons are learnt.

The Incident Management Procedures set out how Gaddum will investigate and manage information and incidents; and provide staff with guidelines on identifying and reporting information incidents, including near-misses.

4.1 Scope

The procedures apply to incidents that impact on the security and confidentiality of personal information. These information incidents can be categorised by their effect on service users and their information:

- Confidentiality;
- Integrity;
- Availability.

These procedures apply to all Gaddum staff.

4.2 Managing Incidents

All service managers have been assigned the role of incident manager for their respective projects, and they will report any incidents to the information governance lead.

Any actual or potential information incident in the service will be assigned to one of the following categories and investigated and managed accordingly.

4.3 Report that service user confidentiality has been breached or put at risk

- Interview the complainant to establish the reason for the complaint and why the practice is being considered responsible;
- Investigate according to the information given by the complainant;
- Record findings;
- Where necessary, provide written explanation to the service user with a formal apology if warranted;
- Take and document appropriate action.

4.4 Inadequate disposal of confidential material

- Investigate how the information left the service by interviewing staff and contractors as appropriate;
- Consider the sensitivity of the data and the risk to which the service user(s) have been exposed;
- Consider whether the service user(s) should be informed and, where the breach is likely to result in a risk for the rights and freedoms of individuals effected, Gaddum must by law contact the individuals effected without undue delay;
- Record findings;
- Take and document appropriate action.

4.5 Attempted or actual theft of equipment and/or access by an unauthorised person

- Check the asset register to find out whether equipment is missing;
- Investigate whether there has been a legitimate reason for removal of equipment;
- If the cause is external inform the police, ask them to investigate and keep them updated with your findings;
- Interview staff and check the asset register to establish what data was being held and how sensitive it is;
- Establish the reason for the theft/unauthorised access, if possible;
- Consider whether there is a future threat to system security;
- Inform insurers;
- Review the physical security of the centre;
- If there has been unauthorised access to the practice computer system:
  - Ask the system supplier Yellow Grid to conduct an audit to determine whether unauthorised changes have been made to service users records;
  - Check compliance with access controls procedures
- Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate;
- If computer hardware or the core software has been stolen, inform the system suppliers to enable restoration of system data to new equipment;
- Record findings;
- Take and document appropriate action.

4.6 Computer misuse by an authorised user

- Interview the person reporting the incident to establish the cause for concern;

- Establish the facts by:
  - Asking the system supplier to conduct an audit on activities by the user concerned;
  - Interviewing the user concerned.
- Establish whether there is a justified reason for the alleged computer misuse;
- Consider the sensitivity of the data and the risk to which the service user(s) have been exposed;
- Record findings;
- Take and document appropriate action.

4.7 Lost or misfiled service user records

- Investigate who last used/had the paper record by interviewing staff and contractors as appropriate;
- Consider whether any care has been provided based on incorrect information within a service user record;
- Consider whether service user care has been delayed due to information not being available;
- Establish whether missing information can be reconstituted e.g. from electronic records;
- If information within records has been misfiled, ensure it is restored to correct filing order/returned to correct record;
- Where necessary provide a written explanation to the service user with a formal apology;
- Record findings;
- Take and document appropriate action.

4.8 Reporting Incidents

If you discover something that could be considered as an incident you should report it to your service manager and complete an incident reporting form. This should then be sent to the Information Governance lead.

In instances where a breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, we are obligated to inform the person/persons affected without undue delay (and no more than 72 hours from the discovery of the breach). All incidents must then be reported to the Information Governance who will inform the ICO.

Your Information Governance lead will investigate the incident and may wish to speak to you directly as things progress.

All registered incidents are re-evaluated after a 6-month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those type of incidents has reduced. If there is no change in the volume of each type of incident the senior management are alerted and appropriate action taken.

5. Data Protection

This policy highlights the six data protection principles for processing Data under the General Data Protection Regulation (GDPR). It outlines how we adhere to and implement the principles, and demonstrates Gaddum's commitment to meet legal obligations as laid down by GDPR and to protecting the individual's data.

Gaddum will:

- ensure that all staff are made aware of their responsibilities to the protection of data through relevant documents and training
- regularly review data protection procedures and guidelines within the organisation

5.1. <u>The data protection principles of processing:</u>

- **Processed lawfully, Fairly and in a transparent manner**

Under the individual's right to be informed, Gaddum will supply information to the individual regarding all of their rights and the processing of their data.

- **Collected for the specified, explicit and legitimate purpose**

Internal documentation will highlight our lawful basis for processing data, and which data we may need to gain consent to process. Any information where consent is our lawful basis must obtain expressed and personal consent form the individual and remain aware that the information should not be processed in future where consent for the processing of this information is withdrawn by the individual.

- **Adequate, relevant and limited to what is necessary**

Through data minimisation, the data requested of an individual will be limited to that which will help with the provision of a service. Some information is required by funders or commissioners where other information may be useful for understanding the individual's situation. All data will have been assessed by the Data & Performance coordinator and each service manager to ensure that data retained is adequate, relevant and necessary.

- **Accurate and, where necessary, kept up to date**

In conjunction with Article 13(2b) of the General Data Protection Regulation, at the time of obtaining personal data Gaddum will inform the individual of their right to rectification, erasure of personal data, the right to restrict processing and to object to processing data as well as the right to data portability.

- **Retained only for as long as necessary**

For the majority of services, data is retained for seven years after the individual has stopped working with us. This is to ensure it is available for Subject Access Requests, and to potentially defend possible future legal claims for the individual and Gaddum. In the cases of young persons, where the person is under the age of 16 when they begin working with us, it is required that we keep the information until the age of 25 (7 years from their 18th birthday). This is required for such instances where child protection may be involved or require information on a young person's case.

- **Processed in an appropriate manner to maintain security**

Gaddum will have documentation outlining how data is processed for each service ensuring that risks are identified and managed. The safe transfer of data policy highlights the potential risks to data and how we should transfer it securely when working with third parties or providing information to commissioners.

5.2. Lawful Bases for Processing

In relation to any processing activity Gaddum will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
  - that the data subject has consented to the processing;
  - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - that the processing is necessary for compliance with a legal obligation to which the Company is subject;
  - that the processing is necessary for the protection of the vital interests of the data subject or another natural person; [or]
  - [that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or]
  - that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph □o below), and document it; and

- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interests' assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant privacy notice(s).

5.3. Sensitive personal information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

- Gaddum may from time to time need to process sensitive personal information. We will only process sensitive personal information if:
  - we have a lawful basis for doing so as set out in the paragraph above, e.g. it is necessary for the performance of the employment contract, to comply with legal obligations or for the purposes of the Gaddum's legitimate interests; and
  - one of the special conditions for processing sensitive personal information applies, eg:

  a) the data subject has given has given explicit consent;

  b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

  c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

  d) processing relates to personal data which are manifestly made public by the data subject;

  e) the processing is necessary for the establishment, exercise or defence of legal claims; or

  f) the processing is necessary for reasons of substantial public interest.
- Before processing any sensitive personal information, staff must notify the IG Lead of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.
- Sensitive personal information will not be processed until:
  - an assessment has taken place; and

    - the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

- Gaddum will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.
- **During the recruitment process**: the HR department, will ensure that (except where the law permits otherwise):
    - during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;
    - if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
    - any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;
    - 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
    - we will **[**not ask health questions in connection with recruitment OR only ask health questions once an offer of employment has been made**]**.
- **During employment**: the HR department will process:
    - health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;
    - sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting **(**Where possible, this information will be anonymised**)**; and
    - trade union membership information for the purposes of staff administration and administering 'check off'.

5.4. Criminal records information

Criminal records information received by Gaddum may be retained for risk assessment purposes

5.5. Privacy Notice

Gaddum has produced a Privacy Statement online for our service users, which provides information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This statement outlines the personal information we collect, how it is used and for what purposes.

5.6. Individuals Rights

Under the General Data Protection Regulations, Individuals have control over the data they supply and how it is used. To ensure you can exercise the rights of the individual correctly, and understand your own rights, please read "**Exercising the Rights of the Individual**" document.

6. Access Control Procedures

Technical access controls are built into information systems by our IT systems provider. To ensure confidential information is protected, this functionality must be supported by operational and managerial controls put in place by Gaddum.

The Access Control Procedures set out how Gaddum will allocate, manage and remove access rights to computer systems holding service user information so that only authorised personnel have access to use and share information held within those systems; and they aim to ensure that access rights are used appropriately by Gaddum staff.

6.1. Scope

These procedures relate to access controls for computer-based information systems managed by Gaddum to store service user identifiable data. They therefore cover the allocation, management and removal of user accounts and the guidelines provided to Gaddum staff to ensure they use the service-managed system appropriately.

6.2. Summary of technical access controls

Gaddum utilises Microsoft Windows Active Directory profile management ensuring users only have access rights relevant to the AD Group they are members of. Users are required to login into the domain using a username and password in order to gain access to the server and files. Access to Gaddum server is limited to users located within Gaddum network and the IT provider. Email Access is provided via Microsoft Office 365 E1 plan which is hosted in Microsoft Azure platform.

6.3. Responsibility for user access management

Gaddum has assigned Service Managers with the responsibility for determining user access rights to the system. However, Yellow Grid must administrator these rights, and as such need to be informed of requirements for new employees or changes to existing employees access to sensitive areas. The unnecessary allocation and use of administrator rights is often found to be a major contributing factor to the vulnerability of systems that have been breached, therefore allocation of administrator rights to other staff can only be authorised by the Service Managers.

6.4. General

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. During their induction to the system each user is given a copy of guidelines for staff on use of the system and their user login details, and is required to sign to indicate that they understand that they understand the conditions of access. A record is kept of all users given access to the system.

6.5. New permanent staff

When a new employee joins the service the service manager arranges access to the system.

6.6. Locum staff

Temporary access is granted on a need to use basis. Such logons are assigned Yellow Grid at the request of Service Managers. Temporary logons are identified by a specific logon and are time limited and are deleted or suspended immediately when no longer required.

6.7. Change of user requirements

Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account, e.g. if the user is on long-term leave, or a locum who returns to the practice sporadically. Requests are made to the Service Managers and a record is kept of all changes.

6.8. Password management

The service system has the following password protection features:

- Users must change their password after the first logon;
- User must select complex passwords (must contain letters and numbers);
- Users must change their passwords periodically (every 3 months);
- Prevention of password re-use (user cannot reuse one of their last 3 passwords);
- Users may change their password at their own request.

6.9. Forgotten password

Where a user has forgotten her/his password, a replacement should be requested from the Service Managers, who issue a temporary, single use, password which requires the user to reset their password to one they are more likely to remember.

6.10. Removal of users

As soon as an individual leaves the centre, all their logons are revoked. As part of the employee termination process project managers inform their

Service Manager of all leavers and their date of leave. This also applies to self-employed contractors.

6.11. Review of access rights

The Service Managers review all access rights on a regular basis, or at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons, which are identified, are disabled immediately and deleted unless positively reconfirmed.

6.12. Monitoring compliance with access rights

The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that service staff are complying with their duty to use their access rights in an appropriate manner. Areas considered in the compliance include whether:

- Only staff regularly working in the service are registered as active users on the system;
- Allocation of administrator rights is restricted;
- Access rights are regularly reviewed;
- Staff are appropriately logging out of the service system.

7. Handling Security Incidents Procedure

There are several ways in which service user confidentiality may be breached such as theft, break-ins, and poor disposal of confidential waste. All breaches should be investigated and reported accordingly. This guidance suggests mechanisms for handling security incidents where service user confidentiality has been or may have been breached.

The majority of data security breaches are innocent and unintentional such as leaving your computer ‘unlocked’ when you leave your desk. However, ‘near misses’ where no actual harm results from the incident, should still be reported and analysed to look for possible ways of preventing an actual incident occurring in the future.

7.1 Definitions

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data security incident could be defined as:

- The disclosure of confidential information to any unauthorised individual;
- The integrity of the system or data being put at risk;
- The availability of the system or information being put at risk,

An adverse impact can be defined for example as:

- A threat to personal safety of privacy;
- A legal obligation or penalty;
- A financial loss.

If the breach is likely to result in a risk to the rights and freedoms of the individuals effected, Gaddum must by law contact the individuals effected without undue delay, to detail the data breach and outline our next steps with regards to protecting the rights of the individual.

7.2 Types of Security Incidents

The types of security incidents likely to affect service user confidentiality are variable. Data security incidents may take many forms including the following:

- Theft of equipment holding confidential information e.g. laptops, client files.
- Unauthorised access to a building or areas containing unsecured confidential information.
- Access to service user records by an unauthorised user who has no work requirement to access the records.
- Authorised access which is misused.
- Electronic access via hacking or viruses.
- Misuse of equipment such as the internet on PCs, text messages on mobiles and e-mails.
- Inadequate disposal of confidential material e.g. paper, hard drive, laptop or desktop
- Car theft/break-ins which may contain a laptop or paper files with confidential data
- Unauthorised access to records away from premises (e.g. laptops and client notes.)
- Complaint by a service user, or a member of the public, that confidentiality has been breached.
- Careless talk (for example discussing an individual’s case in an open space where people could overhear and identify the individual).

7.3 Data Security Incident Monitoring

A data security incident may come to light because a service user has complained about a breach of confidentiality or because of one of the above incidents.

In the first case the cause of the breach will need to be investigated by interviewing the service user, interviewing staff and checking incident logs and computer audit trails. There may also be opportunity to investigate CCTV videos.

In the second case the risk to service user confidentiality should be assessed and any damage limitation may need to be applied. In cases where a breach of security could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, it will be appropriate to warn service users of the breach to their confidentiality.

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible.

Because of the variety of different types of security incident it is important to have clear procedures in place to cover the main types of incident. Any investigations may involve a number of key individuals. The investigation should be co-ordinated by the information governance lead Sam Palmer, who will decide how to take matters forward/resolve them. All staff should be aware of the need to report any suspicious incidents to the named individual.

Staff must understand the reporting procedures and the type of incidents to report. Near misses are indicators of potential problems and should also be reported. In order to respond fully to an incident, audit logs need to be kept.

A log should be kept of all incidents reported whether they lead to a complaint or not. All incidents should be considered as to whether they indicate a need for improvement in arrangements. The log may be incorporated in other incident logs as appropriate. A regular report on the number, type and location of data security incidents should be made allowing any trends to be picked up and addressed.

7.4 Reporting Arrangements

All incidents or information indicating a suspected or actual data security breach should initially be reported to the immediate project manager and then a completed incident form sent to the information governance lead, who must keep a record of all incidents that are reported. The record need not be more than a statement of the persons involved in the incident, a description of the incident and what action has been taken. The information incident reporting form is intended to be used for this.

Where the suspected security breach involves the staff members’ project manager, the individual should inform their project manager’s superior or when necessary the Chief Executive.

If a staff member believes a security breach is the result of an action or negligence on behalf of the Chief Executive, the incident should be reported directly to a Trustee.

Where there has been an incident involving an IT system, the information governance lead and our IT services Yellow Grid (when necessary) must be informed to determine whether an actual security breach has taken place. The majority of IT security breaches are innocent and unintentional and would not normally result in disciplinary action being taken.

If an actual data breach has occurred, the incident should be reported immediately to the information governance lead.

It may also be necessary to report the incident to others depending on the type of likely consequences of the incident (for example informing the individual if a breach of security could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed).

7.5 Incident Classifications

Incidents should be classified according to severity of risk, as follows:

1 = High risk of harm to service users whose confidentiality has been breached

2 = Intermediate risk of harm to service users whose confidentiality has been breached

3 = Low risk of harm to service users whose confidentiality has been breached

The senior managers in Gaddum should review the number and type of security incidents, which have occurred, regularly and decide on any appropriate preventative action to be taken.

7.6 Procedure for dealing with various types of Incident

All staff at Gaddum have a responsibility to ensure that their laptops, and PC's are free of confidential Information. Where possible, they should make use of their own space on the Server in order to save documents that could be considered confidential. However, if there has been a Theft of equipment holding confidential information – PCs, laptop, and client notes etc., and unauthorised access to an area with unsecured confidential information:

- Check the asset register to find out which equipment is missing.
- Investigate whether there has been a legitimate reason for the removal of the equipment.
- If the cause is external, inform the Police and ask them to investigate.
- Interview staff to establish what data was being held and how sensitive it is.
- Establish the reason for the theft/unauthorised access.
- Consider the sensitivity of the data and the risk that it will be misused, in order to assess whether further action is appropriate.
- Consider whether there is a future threat to system security.
- Inform organisations of replacement requirements, this would be Yellow Grid.

- Inform system suppliers if appropriate.
- Follow the reporting arrangements above.

Access to service user by an authorised user who has no work requirement to access the record:

- Interview the person reporting the incident to establish the cause for concern.
- Establish the facts.
- Establish the reason for unauthorised access.
- Consider the sensitivity of the data and the risk to which the service user(s) have been exposed and consider whether the service user(s) should be informed.
- Take appropriate disciplinary action.
- Follow the reporting arrangements above.

Inadequate disposal of confidential material (paper, PC hard drive)

- Investigate how the electronic or paper data left the building by interviewing staff and contractors as appropriate.
- Consider the sensitivity of the data and the risk to which the service user(s) have been exposed and consider whether the service user(s) should be informed.
- Take appropriate action to prevent further occurrences.
- Follow the reporting arrangements above.

Procedure for dealing with complaints about service user confidentiality by a member of the public, service user or member of staff:

- Interview the complainant to establish the reason for the complaint and why Gaddum is being considered responsible.
- Investigate according to the information given by the complainant and take appropriate action.
- Follow the reporting arrangements above.

8. Record Management

Record management is the responsibility of all Gaddum staff. It is of paramount importance that the records are created, handled and stored appropriately as they contain confidential personal information about our Service Users. The misuse/mishandling of service user records is regarded as a data breach and could result in legal action.

Manual files containing personal identifiable information must be kept in locked and secure storage. Confidential information should not be left on desks unattended and electronic records should not be left open on computers unattended. All computers must be locked by the user when leaving them unattended.

Records should not be removed from the premises unless authorised by the manager of the service, deemed as absolutely necessary and a risk assessment has been undertaken. Any records that have been authorised to be taken out of the premises must be kept secure at all times and returned to the office as soon as possible. Gaddum will provide lockable bags if required to ensure the records are kept as secure as possible. If working on public transport workers should risk assess their surroundings as to the level of confidentially and where possible ensure that they are not overlooked if working on a laptop, or overhead, if making telephone calls. Any breaches in record management will be reviewed by the IG Lead and could result in a disciplinary proceedings based on the level of the risk.

8.1 Staff Responsibilities

Staff should act as advocates for service users in all matters relating to recording information. Service users can often be powerless and vulnerable. Therefore, staff must be proactive in defending the interests of the service users by protecting their personal information.

8.2 Record Keeping

Permanently kept records should contain factual material only. No interpretation is to be included, except where it is cited as a reason for a professional decision. In this case, it must be made explicit that it is the professional judgement of the worker and the evidence should be given for that judgement.

8.3 Recording Information

Recorded material should be kept to a minimum consistent with accountability and continuity. The minimum factual information excepted is:

- Name (unless it is to be kept anonymous under specific contractual agreement)
- Address
- Service users description of ethnicity
- Gender
- Age
- Date referred to Gaddum
- Reasons for referral given to Gaddum
- Dates of contact
- Missed appointments
- Decisions or agreements reached (staff must record their actions and reasons regarding situations of risk, abuse or legality)
- Copies or description of any significant contact with other professionals where appropriate

A copy of all letters, reports etc., must be kept on the service user file. If there is no individual service user file, but only a record card in mutual register (e.g.

GP counselling patients) then the worker must have a 'copy letters etc' file which is to be kept at Gaddum offices.

Sometimes, staff will need to produce letters or reports as part of the health team. A copy of this material must be placed on the medical records.

8.4 Records created for other purposes

Records produced as an 'aide-memoire,' or for supervision, might contain interpretation or speculation. Such records must be kept safely at Gaddum from admin records and produced for a specific purpose only. These records must be shredded once their intended purpose is achieved.

8.5 Working for Gaddum at external sites

Where a worker normally operates for Gaddum, but in another professional setting (e.g. GP surgery counselling) it must be agreed, between the worker, Gaddum manager and the third party, how recordings are to be kept. Normally the contract between the worker and the service user is confidential and will not be recorded on any other records, e.g. medical records. Where for example a GP/another professional is consulted about a matter of medical judgement, risk or legality, a copy of the factual material discussed, advice given, decisions taken and reasons, should be given to the other party to keep for record purposes.

8.6 Open Records Policy

Gaddum operates an 'open' records policy and the right of service users to examine all records originating from Gaddum staff relating to them should be borne in mind. Please note that written information originating from a third party cannot be shown to the service user without the permission of the third party.

Service users must have the recording policy explained to them on first contact (if it is possible.) They must be made aware at the first opportunity, of what information is kept about them, where it is kept, who might see it and their right to see it for themselves.

Please remember that, except in the very clear circumstances where service users have rights and obligations as detailed above, questions about disclosure and confidentiality can be difficult and staff should seek help and support from their project manager or the information governance lead, if necessary.

9. Data Retention and Deletion/Disposal policy

The General Data Protection regulation states that data should not be retained for longer than is necessary for the purpose of which it was obtained.

This translates to the end of the service currently provided to the service user. However, we do keep information for longer than that period of time, up to eight years in many cases from the end of the service being provided. This time frame may be increased further for information which has been assessed and deemed necessary. For a full retention schedule and for further information, please refer to the “**Data Retention and Disposal/Destruction Policy**” document.

10. Associated Policies

- Adverse incidents procedures
- Business Continuity Policy
- Casework guidance
- Employee Handbook
- Internet and social media guidelines
- Mobile phone policy
- Safeguarding policy
- Risk Management
- Data Retention and Disposal/Destruction Policy
- Exercising the Rights of the Individual Policy