Ball Tree Surgery

Data Security Policy

1. Introduction

1.1. This Data Security Policy is ***Ball Tree Surgery's*** (hereafter referred to as "us", "we", or "our") policy regarding the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality).

2. Purpose

2.1. The purpose of this document is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

2.2. This Data Security Policy covers:

2.2.1. Physical Access Procedures;

2.2.2. Digital Access Procedures;

2.2.3. Access Monitoring Procedures;

2.2.4. Data Security Audit Procedures;

2.2.5. Data Security Breach procedures.

3. Scope

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

3.2. This policy applies to all staff, including temporary staff and contractors.

4. Physical Access Procedures

4.1. Physical access to records shall only be granted on a strict 'Need to Know' basis.

4.2. During their induction each staff member who requires access to confidential information for their job role will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation.

4.3. Our staff must retain personal and confidential data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets and doors.

4.4. All Locations, when left unoccupied, must be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage. G**uidance on how to implementing clear desks: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/clear-desk-and-screen.**

4.5. The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

4.6. We will risk assess each storage location to ensure that the data is properly secured. This risk assessment forms part of the IAR.

4.7. A record will be kept of who has access to each storage location. This record can be found ***Ball Tree Matrix***

4.8. An audit will be completed at least annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit Procedures [7] below.

5. Digital Access Procedures

5.1. Access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.

5.2. We will ensure that each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.

5.3. The use of group IDs is only permitted where they are suitable for the work carried out.

5.4. During their induction each staff member who requires access to digital systems for their job role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access.

5.5. A record is kept of all users given access to the system. This record can be found ***Ball Tree Matrix***

5.6. In the instance that there are changes to user access requirements, these can only be authorised by the Data Protection Champion **or equivalent job role**.

5.7. The IAR will contain the location of all confidential and sensitive personal information which is digitally stored.

5.8. We will follow robust password management procedures and ensure that all staff are trained in password management. G**uidance on password management and a password policy here: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/passwords/example-policy and here: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach**

5.9. As soon as an employee leaves, all their system logons are revoked.

5.10. As part of the employee termination process the Data Protection Champion **or equivalent job role** is responsible for the removal of access rights from the computer system.

5.11. The Data Protection Champion **or equivalent job role** will review all access rights on a regular basis, but in any event 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.

5.12. When not in use all screens will be locked and a clear screen policy will be followed. **There is guidance on clear screen policies here: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/clear-desk-and-screen]**

6. Access Monitoring Procedures

6.1. The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

6.2. Areas considered in the compliance check include whether:

6.2.1. Allocation of administrator rights is restricted;

6.2.2. Access rights are regularly reviewed;

6.2.3. Whether there is any evidence of staff sharing their access rights; **staff should know that this is can result in disciplinary procedures unless you specifically allow this in your organisation**

6.2.4. Staff are appropriately logging out of the system;

6.2.5. Our password policy is being followed;

6.2.6. Staff understand how to report any security breaches.

7. Data Security Audit Procedures

7.1. Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether

confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme. **How frequently you audit information can vary, but as a minimum there should be a full annual audit.**

7.2. Audits will be carried out as required by some or all of these methods:

7.2.1. Unannounced spot checks to random work areas;

7.2.2. A series of interviews with management and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by **a Practice Manager**;

7.2.3. Based on electronic reports. **This can be from your ICT contractor or from internal monitoring.**

7.2.4. Based on electronic reports from care planning software or auditing of care plans. **This can be from your ICT contractor or from internal monitoring.**

7.3. The following checks will be made during data security audits: **note that you should select which of these you undertake as part of your auditing process**

7.3.1. The Information Asset Register has been reviewed, updated and signed off;

7.3.2. The Record of Processing Activities has been reviewed, updated and signed off;

7.3.3. Failed attempts to access confidential information;

7.3.4. Repeated attempts to access confidential information;

7.3.5. Access of confidential information by unauthorised persons;

7.3.6. Previous confidentiality incidents and actions, including disciplinary, taken;

7.3.7. Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;

7.3.8. Appropriate communications with service users;

7.3.9. Appropriate recording and/or use of consent forms;

7.3.10. Appropriate allocation of access rights to confidential information, both hardcopy and digital;

7.3.11. Appropriate staff access to physical areas;

7.3.12. Storage of and access to filed hardcopy service user notes and information;

7.3.13. Correct process used to securely transfer personal information by post, fax or email **as appropriate**;

7.3.14. Appropriate use and security of desk and mobile devices in open areas;

7.3.15. Security applied to PCs, laptops and mobile electronic devices;

7.3.16. Evidence of secure waste disposal;

7.3.17. Appropriate transfer and sharing arrangements are in place;

7.3.18. Security and arrangements for recording access applied to manual files both live and archive, *e.g.* storage in locked cabinets/locked rooms.

7.3.19. Appropriate staff use of computer systems, *e.g.* no excessive personal use, no attempting to download software without authorisation, use of social media, attempted connection of unauthorised devices etc. **this should match what your organisation has deemed as acceptable use.**

8. Data Security Breach Procedures

8.1. In order to mitigate the risks of a security breach we will:

8.1.1. Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures;

8.1.2. Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach;

8.1.3. Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place.

8.2. In the instance that it appears that a data security breach has taken place:

8.2.1. The staff member who notices the breach, or potential breach, will complete a Data Security Breach Incident Report Form without delay;

8.2.2. This form will be completed and handed to the Data Protection Champion **or equivalent job role** or, if they are not available, to a member of senior management;

8.2.3. The Data Protection Champion will complete the rest of the Incident Report Form and conduct a thorough investigation into the breach;

8.2.4. In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk/incidents/);

8.2.5. As part of our report we will provide the ICO with the following details:

8.2.5.1. The nature of the personal data breach (i.e. confidentiality, integrity, availability);

8.2.5.2. The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);

8.2.5.3. The categories and approximate number of personal data records concerned;

8.2.5.4. The name and details of our Data Protection Champion **or equivalent job role**;

8.2.5.5. The likely consequences of the breach;

8.2.5.6. A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

8.2.6. The Data Protection Champion will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay;

8.2.7. A data security breach must be marked on the IAR and will prompt an audit of all processes in order to correct any procedure which led to the breach;

8.2.8. A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

9. Responsibilities

9.1. **Practice Manager** is responsible for physical security;

9.2. **Practice Manager** is responsible for updating and auditing the IAR and ROPA;

9.3. **Practice Manager** is responsible for digital access;

9.4. **Practice Manager** is responsible for managing breaches;

9.5. **Practice Manager** is responsible for data security audits.

11. Approval

11.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	Gerard Cronin
Signature	
Approval Date	05/03/2019
Review Date	Annual

Appendix: Data Security Audit Checklist

This checklist is a guide which you might chose to use – you can add or remove these checks from your audits as applicable for your organisation.

Staff	**Date audited**
Spot check that staff understand their responsibility towards data security	
Spot check that staff are aware of our data protection policies	
Have staff received training on data protection?	
Have any staff undergone disciplinary action in relation to data protection and security?	
Spot check that staff understand how to report security breaches and near misses.	
Physical Access to hardcopy records	
Check the record of which staff have access to confidential areas is up to date.	
All offices, files, or cabinets which contain confidential information are kept locked when not in use.	
Has all confidential waste been disposed of securely and are there destruction certificates? (If applicable)	
Has anyone inappropriately accessed, or attempted to access, confidential records?	
Digital Access to records	
Is the allocation of administrator rights restricted?	
Have staff access rights been reviewed?	
Check if there is any evidence of staff sharing access rights.	
Screens are locked when not in use.	
Check that our password policy is being followed	
Has anyone inappropriately accessed, or attempted to access, confidential records?	
Have appropriate security measures been applied to all computers, laptops and mobile devices?	
Staff are using computers appropriately e.g. no personal use, no downloading unapproved software, no social media use etc.	
Sharing data	
Our procedures for safely sharing personal information via post are being followed.	
Our procedures for safely sharing personal information via fax are being followed.	
Our procedures for safely sharing personal information via secure email are being followed.	
Legal Checks	
The Information Asset Register has been reviewed and signed off.	
The Record of Processing Activities has been reviewed and signed off.	
Records of consent are up to date and still applicable.	