Cordis Bright | Information Governance and Data Protection Policy

Table of contents

Overview

Introduction

1. The Information Governance and Data Protection Policy sets out the standards to be applied across Cordis Bright for managing information governance and data protection including the organisational arrangements, roles, responsibilities and policies.

2. It is designed to cover the framework of law and best practice to ensure information is managed in a confidential, secure and consistent way. Particular focus is placed on the management of personal data and other confidential information to ensure it is handled legally, securely and efficiently.

Policy statement

3. Cordis Bright is committed to managing its information – and those of its clients where we act as a data processor – securely, legally and effectively. This policy provides guidance to staff around how information should be managed and outlines the accountability structures, governance processes, documented policies and procedures, staff training and resources required to undertake this task.

4. Good information governance and data protection ensures that Cordis Bright is able to provide the right service, at the right time for the right people in an inclusive, open and accountable way that upholds the rights of individuals.

Scope

5. This framework applies to all Cordis Bright staff and the following groups of people who work for or on behalf of Cordis Bright: non-executive directors, sub-consultants, agency workers, interns, and volunteers.

6. It applies to management and governance of all information across Cordis Bright with a particular emphasis on personal and confidential information. It applies to information held in both electronic and paper format and their associated systems.

Aim

7. The aim of the Information Governance Framework is to ensure that there is a clear structure in place for managing information governance across Cordis Bright and this is communicated to our staff and stakeholders. It will ensure that Cordis Bright is managing all information in an effective and efficient way and is meeting its legal and ethical requirements, including to safeguard the confidentiality and privacy of individuals.

Objectives

8. The objectives of the Information Governance Framework are:

    a. To ensure that Cordis Bright's approach to information governance goes beyond legal compliance, seeking to respect and promote effective protection of personal data in line with the company's ethos, ethics and research governance framework.
    b. Cordis Bright is making the best use of the information it holds to provide the best possible service to staff and clients.
    c. Cordis Bright is protecting personal information to ensure that the confidentiality and privacy rights of individuals are upheld.
    d. Cordis Bright is meeting its legal and statutory duties including in relation to the Data Protection Act/General Data Protection Regulations 2018 or any subsequent legislation to the same effect, the Freedom of Information Act, the Human Rights Act and in upholding the common law duty of confidentiality.
    e. There is a strong senior oversight of information governance within Cordis Bright with a clear reporting structure to the Board.
    f. All Cordis Bright staff and other relevant stakeholders understand the required standards for managing information and are clear about their individual responsibilities in this area.
    g. There are adequate policies, procedures and processes in place to meet the aims of the Information Governance Framework and these are applied consistently across the organisation.
    h. There is a clear structure for managing information risk across the organisation.

Principles of the General Data Protection Regulations (GDPR)/Data Protection Act (DPA) 2018

9. There are six principles of the GDPR/DPA 2018:

    a. Lawful, fair and transparent processing – this principle emphasises transparency for data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organisation or what data the organisation has about them that information needs to be available.

    b. Purpose limitation – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place.

    c. Data minimisation – this principle instructs organisations to ensure the data they capture is adequate, relevant and not excessive. Organisations must be sure that they are only storing the minimum amount of data required for their purpose.

    d. Accurate and up-to-date – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing.

    e. Kept for no longer than necessary – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places.

    f. Appropriate security measures – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilizing dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware.

Roles and responsibilities

Managing Director

10. Overall accountability for procedural documents across the organisation lies with the Managing Director. As the Accountable Officer that has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

11. As part of their exercise of their role, the Managing Director will:

    a. Maintain an awareness of information governance issues.

b. Review and update the Information Governance Framework in line with local and national requirements.
c. Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis.
d. Ensure that line managers are aware of the requirements of the policy.

12. The Managing Director, working with the Office Manager and Cordis Bright's IT support provider, will be responsible for:

a. The formulation and implementation of IT related policies.
b. The creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust IT security arrangements in line with best practice.
c. Effective management and security of Cordis Bright's IT resources, for example, infrastructure and equipment.
d. Developing and implementing a robust IT Disaster Recovery Plan.
e. Ensuring the maintenance of all firewalls and secure access servers are in place at all times.

13. The Managing Director will assume others' roles/responsibilities as detailed below.

Caldicott Guardian

14. Kam Kaur, Director and lead for Safeguarding, has been appointed Caldicott Guardian. She will:

a. Ensure that Cordis Bright satisfies the highest practical standards for handling person identifiable information.
b. Facilitate and enable appropriate information sharing and make decisions on behalf of Cordis Bright following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.
c. Represent and champion Information Governance requirements and issues at Board level.
d. Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.

Data Protection Officer (DPO)

15. The Managing Director has been appointed as Cordis Bright's DPO.

16. The DPO facilitates Cordis Bright's compliance with its legal and ethical obligations in relation to the management of personal information by providing expert advice to the organisation around its duties and responsibilities.

17. The DPO:

a. Advises the organisation of its requirements in relation to the Data Protection Act /General Data Protection Regulations 2018 or any subsequent legislation to the same effect.
b. Monitors the organisation's compliance with meeting the above and the organisation's policies and procedures including the assignment of responsibilities and training of staff and related audits.
c. Collects information to identify what processing the organisation is undertaking.

d. Provides advice in relation to Data Protection Impact Assessments (DPIA) and monitors their performance.
e. Cooperates with the EMT, Board and, if applicable, the ICO and acts as the contact point including ensuring that the EMT, Board and, if applicable, the ICO is consulted in the event that a DPIA shows there is a high risk in a processing activity being undertaken (or proposed to be undertaken).
f. Has regard for and provides advice around risks associated with the processing of personal data.
g. Provides advice, information and issues recommendations to the organisation or any organisation processing information on behalf of Cordis Bright.

Senior Information Risk Owner (SIRO)

18. The Managing Director has been nominated as Senior Information Risk Owner (SIRO) who will:

    a. Take overall ownership of the organisation's Information Risk Policy.
    b. Act as champion for information risk on the Board and provide written advice to the Board on the content of the organisation's statement of internal control in regard to information risk.
    c. Implement and lead the company's Assessment and Management processes.
    d. Advise the Board on the effectiveness of information risk management.
    e. Receive training as necessary to ensure they remain effective in their role as SIRO.

Information Asset Owners

19. For information generated within Cordis Bright, the Managing Director will be the Information Asset Owner. For each project, the designated Project Director will become the Information Asset Owner (IAO). The Managing Director and the Project Directors will:

    a. Lead and foster a culture that values, protects and uses information in an appropriate manner.
    b. Know what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset.
    c. Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.
    d. Understand and address risks to the asset, and providing assurance to the SIRO.
    e. Ensure there is a legal basis for processing and for any disclosures.
    f. Refer queries about any of the above to the Managing Director.

Line Managers

20. Line managers will take responsibility for ensuring that the Information Governance Framework is implemented across teams and individuals that they line manage.

Staff and other relevant stakeholders

21. It is the responsibility of each employee and other relevant stakeholders to adhere to the policy.

22. Staff will receive instruction and direction regarding the policy from a number of sources:

    a. Policy/strategy and procedure manuals.
    b. Line manager.
    c. Specific training course.
    d. Other communication methods, for example, team meetings and peer training.

Executive Management Team and Board

23. The Executive Management Team and Board will oversee and approve the policies and supporting documentation put in place by relevant accountable officers, and review such policies on a regular basis.

Information governance training and awareness

New members of staff

24. As part of their induction, all members of staff will confirm in writing that they have read and understand the full range of policies and guidance in operation across Cordis Bright and have completed the NHS e-learning module on Data Security Awareness.

25. This written confirmation will be held on the employee's HR file.

26. If the employee has any questions and/or feels that additional training is required then they should inform their line manager, who will take appropriate steps. Any training received will be recorded in their HR file for information.

27. These steps should be taken (a) before an employee handles confidential data and/or (b) before completing their probation period (whichever is the soonest).

Ongoing core training

28. Within 12 months of completing their probation and on an annual basis thereafter, each member of staff must:

    a. Re-confirm that they understand the full range of policies and procedures in operation across Cordis Bright.
    b. Confirm that they have re-completed and fully understand the NHS e-learning module on Data Security Awareness.
    c. Confirm whether they need any additional training or support to exercise their responsibilities. If this is required, this will be organised by the relevant line manager. Requests will be responded to in a timely way.

29. Confirmation can be provided via email or in hard copy. This will be recorded in the training log held by the Office Manager.

Enhanced training

30. On occasions, it may be necessary to implement additional or enhanced training to respond to the requirements of individual projects. This decision will be made by the relevant Project Director in consultation with the Managing Director.

31. If additional training is required, relevant employees will be required to complete the training before undertaking the relevant part of the project.

32. Relevant employees will be required to confirm the completion of the training via email or in hard copy. This will be recorded in a log held by the relevant Project Director.

Enforcement

33. Failure to comply with these requirements will be responded to via Cordis Bright's disciplinary procedure.

Other relevant stakeholders

34. Cordis Bright have procedures to ensure that any third parties employed by the company on an *ad hoc* basis, e.g. contractors, consultants or temporary staff, are also made aware of the policies and are asked to read and confirm their acceptance of the policies relevant to the contract they are working on.

Information assets and information risk management

35. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

36. An information asset is usually a set of information that can be identified as it is used for a specific purpose or function within Cordis Bright. Some examples of information assets:

    a. Staff human resources files.
    b. A database of contacts.
    c. Safeguarding referrals.
    d. Data from clients relating to individual's service use.
    e. Service-user identifiable data held for a specific safeguarding audit.

37. Cordis Bright retains an information asset register which lists where all personal, large personal and sensitive data is held as well as describing how it is stored, who it is shared with, the legal basis for processing, and for how long it is stored. It also identifies any additional risk that may be attached to the information asset and how this will be mitigated.

38. Information Asset Owners are responsible for agreeing any actions to mitigate risk linked to their information assets and ensuring the actions are completed.

39. Any significant information risk that affects the organisation is highlighted to the Managing Director and this forms part of Cordis Bright's Data Security Action Plan.

Information lifecycle management

40. Information lifecycle management refers to the processes and guidelines that all Cordis Bright staff and other relevant stakeholders should use to manage corporate information throughout its lifecycle. It applies to all information, in whatever format, stored in any location, both physical and virtual.

41. There are five phases of the lifecycle: creation, retention, use, maintenance, and disposal. For each phase, the relevant Information Asset Owner must ensure that the questions described in appendix 2 can be answered to an acceptable standard by the company as a whole and by the individual responsible employees or other relevant stakeholders.

42. Staff and other relevant stakeholders should also have due regard to the Guidance on Handling Personal Information and other relevant policies.

Data protection statement

43. Cordis Bright needs to collect, retain and analyse personal confidential information about employees in order to carry out its business and to comply with the law. This policy provides a framework on how Cordis Bright will comply with its duties as a Data Controller.

44. As part of its work, Cordis Bright also acts as a Data Processor for its clients. This data can also contain personal confidential information and is processed by Cordis Bright as part of a contract for services. This policy providers a framework for how Cordis Bright will comply with its duties as a Data Processor.

45. No matter how it is collected, recorded and used, this personal information must be dealt with properly to ensure compliance with GDPR/DPA 2018 and other relevant legislation.

Handling personal and sensitive information

Introduction

46. There are three main types of personal and sensitive information, which are defined by the Information Commissioner's Office as:

    a. Personal data, i.e. data about a member of staff, patient or service user which on its own or in combination could identify an individual, e.g. name, address, postcode, NHS number, email address, date of birth, payroll number, driving licence.

    b. Large personal data, i.e. personal data held in a database of more than 51 people. This could be identifiable data or a dataset that, though it might not be able to identify individuals, its release would damage public or client trust.

    c. Sensitive personal data, i.e. personal data which also consists of information as to racial/ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, or criminal offences. This category can also include information for mapping purposes which may lead to damage or distress if disclosed, e.g. biometrics, DNA profile, fingerprints; bank, financial or credit card details; mother's maiden name; National Insurance number; tax, benefit or pension records; health, adoption, employment, school, social services, housing records; and child protection.

47. This document provides advice/guidance on how to handle different types of data. That said, it is important to exercise your own professional judgement about the appropriate approach. If you have any questions about how to proceed, please liaise

promptly with the relevant Project Director, or the Head of Safeguarding or the Managing Director.

Generating or processing data with high risk to individuals

48. Cordis Bright is committed to conducting Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to the rights and freedoms of data subjects.

49. A DPIA must be conducted in the following situations:

    a. When introducing new processing activities involving personal data.
    b. When making significant changes to existing processing activities.
    c. When implementing new technologies that impact personal data processing.
    d. When processing special categories of personal data on a large scale[1].
    e. When systematically monitoring publicly accessible areas on a large scale.
    f. When processing data in a way that could significantly affect data subjects.

50. If the above situations apply or might apply to a project, implementation of a new process, or plan to modify a current system then the relevant person must initiative a DPIA. In the case of an internal Cordis Bright system, this might be the Managing Director. For a client-facing project, this is likely to be the Project Manager in partnership with the Project Director. A template is provided at IDGP02.

51. In terms of timings, a DPIA should be conducted at a stage when the outcome can genuinely affect the development of a system or process.

52. The outcome of the DPIA should be saved on the relevant folder on SharePoint.

Before generation of personal information

53. Ensure that Cordis Bright has and complies with the legal basis for generating the information (see https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/).

54. Ensure that a designated Information Asset Owner is identified from within Cordis Bright.

55. Ensure that only the minimum necessary fields and datasets are collected. Encourage anonymization where viable.

56. Establish a date when electronic data should be put 'beyond use' and hard copy data destroyed. The default period for both is six years.

57. Ensure that all relevant members of staff and other relevant stakeholders who interact with the data have completed the core training. If required, ensure that they receive any additional training that may be needed to meet the specific needs of the project.

58. Ensure that information is stored and saved in compliance with this policy.

[1] 'Large scale' is not defined by GDPR, but guidance is available at section 3 of https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf.

59. Ensure that relevant records are made in Cordis Bright's Information Asset Register (if appropriate).

Before receipt of personal information

60. Ensure you know who the designated Data Controller is for the client.

61. Confirm with the Data Controller whether an Information Sharing Agreement should be put in place (see separate template for an example). And/or as a minimum seek confirmation from the Data Controller that:

    a. They will only transfer data to us in line with their own data protection and information governance policies. This includes whether a Data Protection Impact Assessment should be completed by them (e.g. if Cordis Bright is being asked to process data for a purpose that was not originally envisaged when the data was originally collected).

    b. The client has confirmed the legal basis for giving Cordis Bright access to the information (see https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/).

    c. The client has confirmed the date that electronic data should be put 'beyond use' and/or hard copy data destroyed, e.g. on project sign-off. The default period is six years.

62. Ensure that only the minimum necessary fields and datasets will be sent to you. Encourage anonymization where viable.

63. Check whether the client has any additional requirements for the storage or processing of data, e.g. use of client laptops for analysis, and implement these as appropriate.

64. Ensure that all relevant members of staff and other relevant stakeholders have completed the core training and any relevant refreshers. If required, ensure that team members receive any additional training that may be needed to meet the specific needs of the project.

65. Agree the mechanism by which the client will forward or provide access to the information. As a minimum, Cordis Bright requires the following:

    a. Via email: data is password protected, password is provided via a different medium (e.g. text or letter or to a different email address). For sensitive personal data, we expect an additional level of security to be used, i.e. secure email (e.g. CJSM or Switch Egress). For data that is not anonymous and/or where individuals can be identified we also recommend that password protection is achieved by using a commercially-available AES 256-bit encryption product like 7-Zip or WinZip.
    b. Via post: recorded, signed for delivery.

66. The exception to this is professional contact details for members of staff working for a client or other stakeholders. In this instance, it is likely that this data is publicly available so less stringent transfer and storage of data is required. This policy recommends:

a. Transfer via non-secure email or non-enhanced mail delivery.
b. Electronic storage in the relevant project file on the F-drive.
c. Hard copy storage in locations without locks.

67. Please note, however, that this data can easily become personal data if, for instance, it is combined with other information about the individual, e.g. date of birth, home address. It may become sensitive personal data if it is combined with information about their background or beliefs or views. This includes staff views that are recorded from fieldwork. In addition, all databases of professional contact details over 51 entries should be considered as large personal data. In all of these circumstances, the data should be treated as detailed in paragraph 9 and other relevant paragraphs.

68. Ensure that relevant records are made in Cordis Bright's Information Asset Register (if appropriate).

On receipt or generation of the data

69. For electronic data:

a. Save it to the Cordis Bright server. Cordis Bright stores data on a Microsoft SharePoint server. Sharepoint is a web-based collaborative platform that integrates closely with Microsoft Office 365. Apart from the advantages it brings to companies operationally in terms of sharing files and working together, it also delivers a very secure working environment, reducing the risk of cyber attacks and hacks that can be experienced by traditional land-based file servers. Using Sharepoint means that our data is hosted on Microsoft servers. Data is always encrypted, whether just being stored or being transmitted between a user and the servers, and there are multiple backups. We're able to specify the geographical location we want our data stored in. User logons require complex passwords, and include 2 factor authentication when a logon is required on a new device. This security is reinforced by the level of access control and privacy offered by Sharepoint – we can control who can see what, down to a user by user, file by file level if necessary. Microsoft's Office 365 services adhere to globally recognised security standards including ISO 27001 and 27018.
b. Ensure that the data remains password protected.
c. Ensure that the password is saved in LastPass (see below for further information).
d. Delete any fields or data that are not necessary for the purposes of the project.
e. Do not save to any unsecure portable devices. This includes laptops and regular USB sticks. In exceptional circumstances an IronKey can be used, but only with the permission of the Project Director and Managing Director.

70. For hard copy data:

a. When not in use, ensure that it is stored in a locked filing cabinet.
b. Do not remove from the office. If removal is required, then this must only be done with permission from the Project Director and Managing Director.

71. You must not duplicate or copy data without the prior permission of the Project Director or Managing Director.

72. Ensure that relevant entries are made to the Information Asset Register.

73. If the client or other external stakeholder fails to follow the agreed process for transferring data then you should inform the relevant Project Director within 24 hours of identifying the breach and agree the appropriate course of action. Typically this would involve:

    a. Destroying the data (i.e. shredding hard copy data; deleting files saved on Cordis Bright server (including deleting from the Recycle Bin); and deleting the email and relevant attachments (including deleting from Trash).
    b. Alternatively and, if appropriate, the relevant data fields could be deleted or in the case of hard copies redacted.
    c. Informing the client in writing that the breach of protocol has occurred and asking them to follow their internal procedures for an information governance incident.

Storing passwords

74. Passwords should be saved on LastPass.

75. To do this:

    a. Visit https://www.lastpass.com/.
    b. Download the free version of LastPass.
    c. Set-up an account using your Cordis Bright email address.
    d. Set-up a master password. Ensure that you do not forget this password (no password recovery is available).
    e. Enter details of the project and password in LastPass.

76. You may need to ask LightPath for support to download the software.

77. If you become no longer employed by Cordis Bright, you must immediately delete your Cordis Bright LastPass account.

78. App-based versions of LastPass are available. If these are free, then you may download this to your Cordis Bright mobile device. However you must not download this app on any personal mobile equipment.

Further circulation

79. Avoid forwarding electronic data internally. Rather refer to the file's location on the server.

80. Passwords, data and/or links to data must not be sent in the same message.

81. Passwords should be agreed with the relevant Project Director and/or Managing Director. In all cases, the password should be sent to the Managing Director (as Senior Information Risk Officer). Those members of the company that need access to the data should also be sent the password. For internal email addresses, this can be done via email. For external staff, this policy recommends using an alternative medium to email, e.g. phone or text.

82. If the data needs to be returned to the client follow the same protocols as detailed in this policy.

83. In instances where Cordis Bright needs to transfer personal data to a third party then members of staff must seek agreement in writing in advance from the Managing Director and, as a minimum, follow the requirements detailed in paragraph 65. In addition, the Data Protection Impact Assessment Policy should be consulted.

Data quality

84. Data quality is a key part of our information system, and all staff members are responsible for implementing and maintaining data quality. The Project Director should be responsible for ensuring that appropriate systems and procedures are in place to validate the completeness, accuracy, relevance and timeliness of data/information. Ultimate responsibility for maintaining accurate and complete data and information lies with the DPO.

Putting data 'beyond use' and/or destroying data

85. We follow ICO guidance on the effective deletion of personal data (https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/practical-methods-for-destroying-documents-that-are-no-longer-needed/).

86. Electronic files should be put 'beyond use' by being deleted from the server and, in turn, from the Recycle Bin.

87. Emails and email attachments should put 'beyond use' by being deleted from Outlook and, in turn, deleted from the Recycle Bin.

88. Data held in hard copy should be destroyed by being shredded.

89. The Information Asset Register should be updated to confirm that this data has been appropriately deleted.

90. To keep information safe and secure, Cordis Bright's server uses a back-up system. However, this means that though electronic information may be deleted from the server it may continue to exist in previous versions of back-ups. It is not possible to delete data from the back-up without deleting all other data held in the back-up. Given this, we follow the ICO guidance on putting electronic information 'beyond use'. This means that we will delete copies of data from the server and the Recycle Bin plus we confirm that for any similar data held in back-ups, Cordis Bright:

    a. is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
    b. does not give any other organisation access to the personal data;
    c. surrounds the personal data with appropriate technical and organisational security; and
    d. commits to permanent deletion of the information if, or when, this becomes possible.

Monitoring and reporting

91. If an external stakeholder raises concerns about the way that Cordis Bright is handling personal data then the information governance incident management procedures should be followed.

92. The Managing Director will undertake spot checks of information governance and data protection on at least an annual basis, using the appropriate tool (see IGDP09). Results of each audit should be recorded in the Information Asset Register and the Data Security Improvement Plan.

Handling subject access requests

Introduction

93. The Data Protection Act 2018 gives individuals (data subjects) a number of rights, including the right to access personal data that an organisation holds about them. This right of access extends to all information held on an individual and includes personnel files, case record files, databases, interview notes and emails referring to the individual.

94. If an individual makes a request to view their information, it is known as a "Subject Access Request".

95. The Act stipulates that the data subject must:

    a. Make the request in writing. We request that any requests are directed to the Managing Director.
    b. Supply information to prove who they are (to eliminate risk of unauthorised disclosure).
    c. Supply appropriate information to help Cordis Bright locate the information they require.

96. Upon receipt of a request, the Managing Director will make a determination, using the guidance below, about whether the request is ‘simple’ or ‘complex’:

‘Simple’ requests

97. Cordis Bright policy is to be open and transparent and, wherever possible, to let the individual have a copy of the information with minimum fuss. Such requests will be handled by the Managing Director or Project Director. When responding to such requests, care will be taken to ensure that we do not inadvertently release third party information without their consent.

‘Complex’ requests

98. There may be some instances when a request for information is more complex, for example:

    a. Request involves locating information from multiple sources.
    b. Request involves the release of contentious information.
    c. Request is one in a series of requests from the same individual.
    d. Request involves the release of third party data for which consent has been refused or cannot be obtained.
    e. The data subject does not want to ask for the information from the department/section that holds it.

99. In such cases, the response will be coordinated by the Managing Director in liaison with staff involved in the case.

Responding to requests

100. Cordis Bright must provide:

    a. Information on whether or not the personal data are processed.
    b. A description of the data, purposes and recipients.
    c. A copy of the data.
    d. An explanation of any codes/jargon contained within the data.

101. Cordis Bright must respond to Subject Access Requests within 40 days.

Third Party Data

102. It will sometimes be the case that responding to a Subject Access Request will lead to disclosure of details relating to some another third party. Such third party information should not be disclosed without first seeking the consent of the third party.

103. If consent cannot be obtained (e.g. the third party cannot be contacted) or is refused, then Cordis Bright needs to consider whether or not disclosure is reasonable, taking into account:

    a. Any duty of confidentiality owed to the third party.
    b. The steps taken to seek consent.
    c. Whether the third party is capable of giving consent.
    d. Any express refusal of consent

104. Decisions will be made on a case by case basis.

105. If Cordis Bright decides that disclosure cannot be made, or that information which could identify the third party should be withheld (e.g. third party details are redacted), Cordis Bright will, wherever possible, follow good practice by providing an explanation for the course of action chosen.

Records management

106. The maintenance of appropriate records is extremely important in the event of a Subject Access Request. Knowing who keeps what and where is central to the effective and efficient retrieval of information.

107. All staff are advised:

    a. To be careful about what personal information they keep (including emails).
    b. To try to only record factual information.
    c. Where it is necessary to record an opinion about an individual, to make sure it is justified and wherever possible backed up with factual evidence.
    d. Not to record anything that they would not wish the data subject to see.
    e. To consider how long the information should be retained and to take steps to delete the information when it is no longer required.

Cordis Bright position on charging for Subject Access Requests

108. The Act permits organisations to charge up to £10 for responding to Subject Access Requests. However, this is unlikely to cover the costs of responding to requests, particularly when it involves locating information from numerous sources or where large volumes of information need to be photocopied and posted. There is no scope within the Act to charge more than £10 and wherever possible, Cordis Bright aims to waive this fee. However if we were to receive numerous requests from one individual, we may consider introducing the fee.

109. There may be other circumstances when a charge is made such as:

    a. The data is difficult to locate or is held in multiple locations.
    b. There are large volumes of data to be supplied.
    c. Consent from several third parties is required

Exemptions

110. There are certain situations where Cordis Bright may not be obliged to release information in response to a Subject Access Request. Examples include:

    a. Data containing information relating to a third party for which consent to release the information cannot be obtained.
    b. Information relating to legal proceedings being taken by Cordis Bright.

Information governance incident management

Introduction

111. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non- compliance, and/or financial costs.

112. This section sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents, to minimise the risk associated with any breach/incident, and to prevent any future breaches. It relates to all personal and special categories (sensitive) data held by Cordis Bright regardless of format.

113. Data security breaches include both confirmed and suspected incidents. An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the company's information assets and/or reputation.

114. An incident includes but is not restricted to, the following:

    a. Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record).
    b. Equipment theft or failure.
    c. System failure.
    d. Unauthorised use of, access to or modification of data or information systems.
    e. Attempts (failed or successful) to gain unauthorised access to information or IT system(s).

f. Unauthorised disclosure of sensitive / confidential data.
g. Website defacement.
h. Hacking attack.
i. Unforeseen circumstances such as a fire or flood.
j. Human error.
k. 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

115. Any individual who accesses, uses or manages Cordis Bright's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (Managing Director).

116. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

117. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (see Appendix 1).

118. All staff should be aware that any breach of legislation may result in Disciplinary Procedures being instigated.

Containment and recovery

119. The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

120. An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

121. The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

122. The LIO will establish who may need to be notified as part of the initial containment and will inform the client, ICO or police, where appropriate.

123. The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and risk assessment

124. An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered/reported.

125. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals or clients, how serious or substantial those are and how likely they are to occur.

126. The investigation will need to take into account the following:

    a. The type of data involved.
    b. Its sensitivity.
    c. The protections that are in place (e.g. encryptions).
    d. What has happened to the data (e.g. has it been lost or stolen.
    e. Whether the data could be put to any illegal or inappropriate use.
    f. Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s).
    g. Whether there are wider consequences to the breach.

Notification

127. The LIO and/or the DPO, in consultation with relevant colleagues will establish whether the client and/or Information Commissioner's Office and/or NHS Data Security and Protection Toolkit incident reporting tool will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

128. Every incident will be assessed on a case by case basis; however, the following will need to be considered:

    a. Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation and GDPR.
    b. Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?).
    c. Whether notification would help prevent the unauthorised or unlawful use of personal data.
    d. Whether there are any legal/contractual notification requirements.
    e. The dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

129. Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

130. The LIO and/or the DPO must consider notifying third parties such as clients, the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

131. A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

132. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

133. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

134. The review will consider:

    a. Where and how personal data is held and where and how it is stored.
    b. Where the biggest risks lie including identifying potential weak points within existing security measures.
    c. Whether methods of transmission are secure; sharing minimum amount of data necessary.
    d. Staff awareness.
    e. Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

135. If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Senior Management Team and/or Board. Any future actions will form part of the Data Security Improvement Plan.

136. If appropriate, additional action should be undertaken via the Serious Incident Requiring Investigation Policy and Procedure.

Data security and protection

137. In order to assure Cordis Bright's compliance with effective practice, the organisation will seek validation on an annual basis for:

    a. Data Protection Act registration: Z7031124 which renews yearly on 11 August.
    b. Cyber Essentials Plus.
    c. NHS Data Security and Protection Toolkit.

Monitoring

138. Compliance with the policies and procedures laid down in this document will be monitored by the Senior Management Team on a periodic basis.

139. The Managing Director is responsible for the monitoring, revision and updating of this document on an annual basis or sooner if the need arises.

Changes and new ways of working

140. Any changes to this policy or other Cordis Bright policies or any changes to or new Cordis Bright processes, policies, projects and/or information assets should result in the activation of a Data Protection Impact Assessment.

Other relevant policies

141. This document should be read alongside the following other policies and procedures that relate to information governance and data protection:

    a. Acceptable IT Usage Policy
    b. Disaster Recovery Plan
    c. Enhanced Disclosure and Barring Services
    d. Risk Management Policy

e. Information Asset Register
f. Serious Incident Requiring Investigation Policy and Procedure
g. Data Security Improvement Plan

Approved by the Board: July 2024

Appendix 1: Data breach report form

Please act promptly to report any data breaches. If you discover a data breach, please notify a member of the Senior Management Team immediately, complete Section 1 of this form and email it to the Data Protection Officer, colinhorswell@cordisbright.co.uk with a copy to the office manager, julieireland@cordisbright.co.uk.

Section 1: Notification of Data Security Breach	
To be completed by person reporting the incident	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident:	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Has any client data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
Section 2: Acknowledge of receipt of notification of Data Security Breach	
To be completed by the Data Protection Officer	
Date received:	
Information on immediate next steps:	
Section 3: Action taken	
To be completed by Data Protection Officer or other relevant member of staff	
Incident number:	
Date:	
Person completing this section:	
Action taken by responsible officer(s):	
Was incident reported to the client? If so, provide further details:	
Follow-up action required/recommended by client:	
Was incident reported to the ICO? If so, provide further details:	
Follow-up action required/recommended by ICO:	
Was incident reported to the police? If so, provide further details:	
Follow-up action required/recommended by police:	
Was incident reported to Data Subjects? If so, provide further details:	
Was incident reported to any other stakeholder? If so, provide further details:	

Appendix 2 – Questions for consideration at each stage of the information management lifecycle

Applying these questions will ensure that the organisation as a whole is creating and capturing information that is fit-for-purpose, reliable and accurate. It will help individual members of staff to keep their corporate information in order and is robust and secure.

Creation

- Are you creating the right information?
- Are the right people creating it?
- Proof of provenance
- Need to know versus duty to share
- Longevity and Preservation
- Who owns the information?

Use and maintenance

- Have you defined the purpose for which your information can be used?
- Have you optimized your information for easy location and re-use?
- Do you know who needs to access your information?
- Is access to your information controlled?
- Is your information safe?

Retention

- Do you know what information is being held and why?
- Do you know how long your information must/should be kept?
- How will you ensure continued access to the information?
- Is your information safe?

Disposal

- Are you disposing of the information in the correct way?
- How is the disposal of information controlled?
- When/where has deleted information really gone?
- Is the process auditable?