|  |  |
| --- | --- |
| **DOCUMENT TITLE:** | **Information Governance Policy** |
| **CATEGORY:** | Governance and Quality |
| **TYPE:** | Policy |
| **VERSION NUMBER:** | v2.6 |
| **LAST REVISED:** | April 23 (BWD section updated) |
| **DUE FOR REVISION:** | September 2023 |
| **OWNED BY:** | Company Lead |

|  |  |
| --- | --- |
| **OUR PRINCIPLES:** | With passion and excellence, Delphi makes a difference to people’s lives by providing innovative and specialist addiction services that lead the way from dependence to freedom. |
| **OUR VALUES:** | We all commit to and care about: going one step further with our clients; our wellbeing as individuals and as teams; and improving and strengthening ourselves and our organisation. |

**Information Governance Policy**

|  |  |
| --- | --- |
| Information Governance is the framework for ensuring and assuring that information is managed legally and safely. | This covers personal information relating to patients/service users and employees/workers, and corporate information such as financial and accounting records, business operational information, and research, audit and reporting information.  Information Governance allows the business to ensure this information is handled legally, securely, and efficiently, to support delivery of the best possible care. It also enables the business to meet requests for information and assists with compliance against the current legislative framework and other applicable codes of practice. |

**Roles and Responsibilities**

|  |  |
| --- | --- |
| Within the organisation there is a need to review and approve policy, and to allocate overall Information Governance responsibilities.  As a clinical organisation, an important role of the Caldicott Guardian is to bridge any gaps between Information Governance and Clinical Governance.  The SIRO ensures compliance with data protection legislation (GDPR) and other relevant legislation and codes of practice. | As a subsidiary of The Calico Group, Delphi Medical’s **Data Protection Officer** is appointed directly by the Group. The Data Protection Officer assists Delphi Medical to monitor compliance, inform and advise on data protection obligations, provide advice regarding data protection impact assessments, and acts as a contact point for data subjects and the Information Commissioner’s Office. The Data Protection Officer reports directly to the highest level of management within The Calico Group.  Delphi Medical’s **Caldicott Guardian and Information Governance Lead** is the Company Lead of Delphi Medical. The **Caldicott Guardian** ensures that all personal information is used legally, ethically, and appropriately, and that confidentiality is maintained. They provide leadership and informed guidance on complex matters involving confidentiality and information sharing, ensuring that Delphi Medical satisfies the highest practical standards. Delphi’s Caldicott Guardian works to 7 guiding principles: (1) justify the purpose;  (2) don’t use personal confidential data unless it is absolutely necessary;  (3) use the minimum necessary personal confidential data;  (4) access to this data should be on a strict need-to-know basis;  (5) everyone with access to this data should be aware of their responsibilities; (6) comply with the law; and  (7) the duty to share information can be as important as the duty to protect confidentiality.  The **Information Governance lead** will facilitate regular review and update of this policy. This will ensure that the risks to our information assets are identified, assessed, and adequately controlled. Review may also take place due to the following occurrences:   * Changes to relevant legislation * Identification of new threats and vulnerabilities * Significant organisational restructuring * Significant change in technical infrastructure.     Delphi Medical’s **Senior Information Risk Officer (SIRO)** and is Delphi’s Head of Governance & Quality, a member of Delphi’s Senior Leadership Team.  The SIRO has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks, and for taking steps to mitigate them. The SIRO ensures that good practice in Information Governance is continually developed and disseminated, and that Information Governance is consistent and of high quality. The SIRO is also responsible for administering the security of Delphi Medical’s information assets.  Each individual information asset has an appointed owner who is responsible for the governance of that particular information asset. Full details of the **Information Asset owners** can be found within the Compliance Plan that forms part of this document. Where there is no appointed owner of a system or workgroup, this role will default to the Caldicott Guardian, who will remain responsible until the SIRO identifies an alternative or more appropriate owner.  Delphi’s **Senior Leadership Team** are committed to ensuring high standards of Information Governance. The team nurture a culture of compliance against relevant legislation by continuously promoting key principles and leading by example.  **All Delphi Medical employees/workers** have a responsibility to operate within Information Governance procedures and follow best practice standards. |

**Training and Assessment**

|  |  |
| --- | --- |
| Delphi Medical completes the NHS Information Governance toolkit (Data Security and Protection Toolkit) on an annual basis.  Training is monitored throughout the year to ensure 100% compliance. | The Toolkit is an online assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards.    As an organisation that has access to NHS patient data, Delphi Medical are required to complete this toolkit to provide assurance that we are practising good data security and that personal information is handled correctly.  Delphi Medical audit Information Governance practice across the business as part of a formal audit programme. Audits are reported at the Managers Meeting and exception reported to the Senior Leadership Team.  Following Information Governance and GDPR training at induction; annual training is mandatory for all Delphi Medical employees. This is monitored by our Corporate Services team and flagged via the reporting structure where necessary. |

**Data Protection**

|  |  |
| --- | --- |
| The General Data Protection Regulations (GDPR) form part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). The provisions of such were applied from 25 May 2018. | The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.  The GDPR (Article 5) sets out seven key principles of data protection:   1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimisation 4. Accuracy 5. Storage limitation 6. Integrity and confidentiality (security) 7. Accountability |
| 1. **Lawfulness, fairness and transparency** | 1. Delphi Medical will always be clear, open and honest about how personal data will be used. Delphi Medical’s Privacy Notice covers how, why, where and for how long data is stored, and is always available to individuals both online and within the reception areas of all Delphi Medical buildings. 2. Delphi Medical identifies the lawful basis for collecting and using all personal data as per Article 6 GDPR. This is done before the processing activity commences and is documented within the compliance plan by the relevant service manager and/or the Head of Governance and Quality. As the individual has a right to be informed of the lawful basis for processing under Article 13 and 14, this information is also included in Delphi Medical’s Privacy Notice. 3. As Delphi Medical process special category data, a condition for processing that data is identified within the compliance plan and Privacy Notice. 4. Delphi Medical ensures that nothing is done with the data in breach of any other laws. This is audited by the Service Managers and Head of Governance and Quality, in addition to the security measures in place (see principle 6). 5. Delphi Medical will only use personal data in a way that is fair and not unduly detrimental, unexpected, or misleading to the individuals concerned. We will consider how the processing may affect the individual’s concerned and justify any adverse impact. This reflects our privacy by design approach to data protection and privacy. |
| 1. **Purpose limitation** | 1. Delphi Medical clearly identifies the purpose or purposes for processing all personal data. The purpose for processing is identified before processing commences and is documented within the public Privacy Notice, and the compliance plan that forms part of this document. 2. Delphi Medical will only use the personal data for a new purpose if: this is compatible with the original purpose; consent is received; or if there is a clear basis in law. 3. Delphi Medical regularly reviews processing activities as part of a formal audit programme, and where necessary, we will update our documentation and Privacy Notice for individuals. |
| 1. **Data minimisation** | 1. Delphi Medical only collects personal data that is required for our specified purposes. 2. Delphi Medical will ensure the data held is relevant, sufficient, and adequate to properly fulfil our stated purpose, and we will not hold more than is needed for that purpose. 3. Delphi Medical will periodically review the data we hold as part of the GDPR audit programme and delete anything that is not needed. This is the responsibility of the relevant service managers and the Head of Governance and Quality. |
| 1. **Accuracy** | 1. Delphi Medical will ensure accuracy of any personal data held and record the data source. 2. Delphi Medical will ensure that data is updated to ensure we are able to properly fulfil our purpose. As a matter of good practice, Delphi Medical staff will follow documented processes to check the accuracy of data. 3. Delphi Medical will clearly identify any matters of opinion within records. 4. Delphi Medical will comply with the individual’s right to rectification (see Information Requests). As a matter of good practice, records of challenges to the accuracy of personal data will be kept. |
| 1. **Storage Limitation** | 1. Delphi Medical knows what personal data is held and why that data is needed. 2. Delphi Medical sets out standard retention periods within information processing documentation (see compliance plan). This includes the justification for the set retention periods for each type of personal data held by the business. 3. Delphi Medical will not keep personal data for longer than needed. Our policies and procedures outline the process for periodically reviewing the data held and erasing or anonymising data when it is no longer needed. 4. Delphi Medical will identify any personal data that needs to be kept for public interest archiving, or statistical purposes. 5. Delphi Medical has appropriate processes in place to comply with individual’s requests for erasure under ‘the right to be forgotten’ (see Information Requests). |
| 1. **Integrity and confidentiality (security)** | 1. Delphi Medical has appropriate security measures in place to protect the personal data held across all areas of the business. These include both technical and organisational measures and enable Delphi Medical to restore access and availability to personal data in a timely manner in the event of a physical or technical incident. 2. Delphi Medical operates processes to test the effectiveness of security measures and will undertake any required improvements in a timely manner. 3. Delphi Medical undertakes analysis of the risks presented by processing activities and uses this to assess the appropriate level of security that we need to put in place. 4. Delphi Medical operates an Information Security measures in conjunction with the IT system provider. 5. Delphi Medical understands that we may also need to put other technical measures in place depending on the type of data processed. 6. Delphi Medical uses encryption and/or pseudonymisation where it is appropriate to do so. 7. Delphi Medical understands the requirements of confidentiality, integrity and availability for the personal data that is processed. 8. Delphi Medical ensures that all data processors used also implement appropriate technical and organisation measures. |
| 1. **Accountability** | 1. Delphi Medical takes responsibility for complying with GDPR at the highest management level, and throughout the organisation, keeping evidence of the steps that are taken to achieve compliance with the legislation. 2. Delphi Medical have adopted appropriate technical and organisational measures to ensure accountability such as:    * Consistently reviewing the IG policy (and amending as necessary).    * Ensuring robust written contracts are in place with organisations that process personal data on our behalf. These contracts are reviewed on a regular basis and include the responsibilities of both parties, the indemnity that has been agreed, and confirm that nothing within the contract relieves the processor of its own responsibilities and liabilities under GDPR. Records are kept up to date and consistently reflect current processing activities.    * Maintaining documentation of our processing activities. These are documented and managed electronically by the Corporate Services team.    * Ensuring appropriate security measures. Delphi Medical operates a robust risk management process, organisational policies, and physical and technical measures. These measures ensure ‘confidentiality, integrity and availability’ of our systems and services and the personal data that is processed within them (see Information Security).    * Recording and reporting personal data breaches. **Data breaches** are reported via Delphi’s robust Incident process. All staff follow the Incident reporting process as a term of their employment. Breaches are notified to the Data Protection Officer who in turn notifies the ICO within 72 hours. If the breach is likely to result in adversely affecting individual’s rights and freedoms that individual will be informed without undue delay. Recording of data breaches is maintained and managed by the Corporate Services team (see Data Breaches).    * Taking a data protection by design and default approach. Delphi Medical adopts a ‘privacy by design’ approach to data protection across all areas of the business. Data protection and privacy issues are considered upfront in everything we do.    * Carrying out data protection impact assessments. Privacy Impact Assessments are completed for major projects that require the processing of personal data. The purpose of these assessments is to assess the level of risk posed by the proposed project. Managers completing a Privacy Impact Assessment should consult with Delphi Medical’s SIRO, who will liaise with the Data Protection Officer. A Privacy Impact Assessment template can be found at the back of this document. 3. Delphi Medical review and update accountability measures at appropriate intervals. 4. Delphi Medical operates within a culture of privacy and this builds trust with individuals whose data we work with. |

**Information Requests**

|  |  |
| --- | --- |
| The GDPR provides the following rights for individuals: | 1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling. |
| **1. The right to be informed** | 1. Individuals have the right to be informed about the collection and use of their personal data. This information is provided within Delphi Medical’s Privacy Notice. The document is regularly reviewed and updated as necessary. 2. As part of the consent process, patients/service users are additionally informed about how and why their personal data will be processed when consent is obtained. |
| **2. The right of access** | 1. The right of access, commonly referred to as Subject Access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information (other supplementary information largely corresponds to the information that we provide via the Privacy Notice). It helps individuals to understand how and why Delphi Medical are using their data, and to check that it is being used lawfully. 2. As the GDPR does not specify how to make a valid request an individual can make a subject access request verbally or in writing. The request does not have to include the phrase ‘subject access request’ or reference any legislation. Furthermore these requests can be made to any part of the organisation (including social media). |
| **3. The right of rectification** | 1. Under Article 16 of the GDPR individuals also have the right to have inaccurate personal data rectified. An individual may also be able to have an incomplete personal data completed depending on the purposes for the processing. This right is closely linked to the obligation under the accuracy principle of the GDPR (Article 5). |
| **4. The right of erasure** | 1. The right to erasure is also known as the right to be forgotten. 2. As the GDPR does not specify how to make a valid request for erasure, an individual can make a request verbally or in writing. The request does not have to include the phrase ‘erasure’ or reference any legislation. Furthermore these requests can be made to any part of the organisation (including social media). 3. The right to erasure is not absolute and only applies in certain circumstances. |
| **5. The right to restrict processing** | 1. Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted Delphi Medical are permitted to store the personal data, but not use it. 2. As the GDPR does not specify how to make a valid request for restriction, an individual can make a request verbally or in writing. The request does not have to include the phrase ‘restriction’ or reference any legislation. Furthermore these requests can be made to any part of the organisation (including social media). |
| **6. The right to data portability** | 1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. 2. This right only applies to information an individual has provided to a controller. |
| **7. The right to object** | 1. Individuals have the right to object to the processing of their personal data in certain circumstances. Individuals are told about their right to object within the Privacy Notice. 2. An individual can make an objection verbally or in writing. |
| 1. **Rights in relation to automated decision making and profiling** | 1. Delphi Medical do not operate any automated decision making or profiling. |

**Information Security**

|  |  |
| --- | --- |
| Information and the IT systems that support it represent an increasingly valuable asset to Delphi Medical as increased reliance is placed upon them.  Delphi Medical therefore seeks to protect its information systems from misuse and to minimise the impact of service breaks. | The Company Lead, DPO and IT Team are responsible for the implementation and enforcement of Information Security, having responsibilities for:   * Ensuring that Information Security is implemented throughout the organisation; developing and enforcing detailed procedures to maintain security * Prevention and detection of viruses and other malicious software * Consequences of Information Security violations * Compliance with legislative and contractual requirements * Ensuring that staff are aware of their responsibilities and accountability for information security * Security education requirements * Business Continuity * Monitoring for actual or potential information security breaches * Monitoring and reporting on the state of information technology security within the organisation. |

**Pseudonymisation**

|  |  |
| --- | --- |
| Pseudonymisation is a method which disguises the identity of patients/service users by creating a pseudonym for each patient identifiable data item.  This allows patient linking analysis needed within secondary uses such as research, audits, commissioning, contract monitoring, and reporting. | The aim of pseudonymisation is to obscure the data sufficiently so that the risk of potential identification is minimised to acceptable levels.  De-identified data should still be used within a secure environment, with staff access on a need to know basis.  To effectively pseudonymise data the following actions must be taken:   * Each field of personal data must have a unique pseudonym. * Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability. For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers. * Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports. * Pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised. * The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines. * Pseudonymised data should have the same security as personal data. |
| Delphi Medical currently operates Pseudonymisation methods in the following instances: | * to referring authorities to match their referrals to our discharge data * Within case studies presented for examples of real work that has been undertaken * With Public Health England in cases of death in service. |

**Data Breaches**

|  |  |
| --- | --- |
| Data breaches are handled in line with Delphi Medical’s incident reporting process (see separate Incident Policy). | Examples of data/security breaches include (but not limited to);   * Loss or corruption of data * The availability of the system or information being put at risk * The integrity of the system or data being put at risk * Finding a printout of patient details on a printer or desk * Losing a laptop with personal information on it * Accessing a computer using someone else’s ID and password * Sending personal data via email, without password protection * Trying to access a secure area using someone else’s access rights * Loss of equipment due to crime or an individual’s carelessness * Finding the doors and/or windows have been broken and forced entry gained to a secure room/building * An email being sent to the incorrect recipient containing personal data * Responding to requests for information without following policy * Leaving personal data on the desktop overnight without locking it away * Giving data to people who are not entitled to know either verbally, written or electronically. |

**Confidentiality Code of Conduct**

|  |  |
| --- | --- |
| All employees, including temporary staff, students, and volunteers, are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work (as per their contracts of employment). | This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection legislation and, in addition, for health and other professionals through their own professions’ Code(s) of Conduct.  This means that employees are obliged to keep any personal identifiable information strictly confidential.  It should be noted that employees also come into contact with non-personal identifiable information which should also be treated with the same degree of care e.g. confidential business information such as service user referral letters, discharge summaries, waiting lists data, consultant’s workloads, clinic lists. |
| Key principles for Employees: | * Never give out information on patients or staff to persons who do not “need to know” in order to provide health care, treatment or employment information * You must have valid consent for sharing need to know information * Requests for information from the Police should always be referred to the relevant service manager or a member of the Senior Leadership team * If you have any concerns about disclosing/sharing patient or staff information, you must discuss with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with you should take the callers details and ring them back when you are satisfied the disclosure or information can take place. * If a request for information is made by telephone always check the identity of the caller and whether they are entitled to the information they request; take a number, verify it independently and call back if necessary * Do not share information with the Media under any circumstances * It is strictly forbidden for employees to look at any information relating to family, friends or acquaintances unless they are directly involved in that patient’s clinical care or with the employees administration on behalf of Delphi. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action * Do not talk about service users or staff in public places or where you can be overheard * Do not leave data unattended at anytime * Although Delphi is a paperless organisation, there are processes that require work from paper-based documents. Paper-based confidential information should always be kept secure, within lockable draws in locked rooms, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time * When disposing of paper-based person identifiable or confidential information always use the ‘Confidential Waste’ bins. Computer printouts should either be shredded or disposed of as paper-based confidential waste * Make sure that any computer screens, or other displays of information, cannot be seen by unauthorised personnel * Computers should be locked when unattended * Faxes should always be addressed to named recipients. Always check the number to avoid misdialling and ring the recipient to check that they have received the fax. If the fax machine stores numbers in the memory, always check that the number held is correct and current before sending sensitive information * Personal data sent via email should always be password protected * PC-based information should not be saved onto local hard drives or onto removable media, but onto the Delphi’s network/SharePoint * Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary * Personal passwords issued to you or created by employees should be regarded as confidential and those passwords must not be communicated to anyone. Passwords should not be written down. Passwords should not relate to you or the system being accessed * No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempt to breach security should be immediately reported to a Senior Manager and may result in a disciplinary action and could lead to criminal action being taken against you * If you are concerned that a colleague may be breaching security or confidentiality you may raise this under Delphi’s Whistleblowing Policy which, ensures your confidentiality will be respected and gives you advice and guidance on how to raise your concern * If you are planning on working from home, ensure you have the right authority to do so, and follow the IT Security rules within this policy * All computer software used with Delphi is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff). It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use * Non-compliance with this code of conduct by any person employed by Delphi may result in disciplinary action being taken in accordance with Delphi’s disciplinary procedure, and could lead to dismissal for gross misconduct. |

**Confidentiality Agreement (Non-Directly Employed)**

|  |  |
| --- | --- |
| Confidential information includes all information relating to Delphi and its service users and employees.  If you are in doubt as to what information may be disclosed, you should check with the Caldicott Guardian. | During the course of your time within Delphi you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of Delphi. This condition applies during your relationship with Delphi and when the relationship ceases.  Such information may relate to service user records, telephone enquiries about service users or staff, electronic databases or methods of communication, use of fax machines, hand-written notes made containing information etc. |
| **I understand that I am bound by a duty of confidentiality and agree to adhere to this Code of Conduct and the requirements of the GDPR.**  Print Name: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Witness Name: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | |

**Privacy Impact Assessment**

|  |  |
| --- | --- |
| **Date of Assessment** |  |
| **Assessor** |  |
| **Service** |  |
| **Name of Process** |  |
| **Purpose of Process** |  |
| **Location of Process** |  |
| **Lawful bases for processing** |  |
| **Where will the data come from** |  |
| **Who is impacted by the processing?** |  |
| **Describe the process workflow** |  |
| **Where will the data be stored** |  |
| **What is the process for deleting data** |  |
| **What risks are there to the data subjects?** |  |
| **What protective measures are/will be put in place?** |  |
| **What additional measures will you put in place?** |  |
| **Date of Review** |  |
| **Submitted to DPO Date** |  |

**GDPR Compliance Plan**

