Data Protection/Confidentiality Policy

Version	**1.4**
Approved by AMT	**01/05/2018**
Approved by GAC	**06/06/2018**
Approved by PHA Board	**11/06/2018**
Review Date	**30/06/2021**

1.0 INTRODUCTION

1.1 Data Protection policy – Background

The ease with which personal information can be passed within Public Health Agency (PHA), often by computer, is an undoubted benefit for patients and clients, for those involved in their care and treatment and in the planning and commissioning of services. However, all those concerned need to be aware of the legal duty to protect the confidentiality of personal information, whether it relates to patients, clients, staff or members.

The PHA recognises that it has a responsibility to respect the individual's rights afforded by the Data Protection Act 2018 and EU General Data Protection Regulation (GDPR). We recognise that there is a legitimate expectation on the part of our service users and staff that their information will be treated as confidential and that sharing of that information will be legitimate, necessary and lawful. This policy is based on that expectation and acknowledges that HSC staff will need to have strictly controlled access to personal information, anonymised wherever possible, to enable the effective and efficient delivery of Health and Social Care Services to the local population within Northern Ireland.

All PHA staff, agents and contractors are reminded of their responsibilities under Data Protection, GDPR legislation and all associated Codes of Practice and governing Principles. Any breach of PHA policy will be treated as a serious matter and may result in disciplinary action including dismissal, or, in the case of an Agent or Contractor, consideration will be given to the review or termination of any formal arrangements.

1.2 Purpose of the Policy

This policy aims to clarify why it is necessary to collect, store or process information, how long information may be stored for and how and when personal information may be shared.

It also addresses the need to make patients, clients and staff aware of the ways in which their information might be used and emphasises the use of anonymised information wherever possible, setting out the circumstances in which information may be passed on for other purposes or as a legal requirement.

It also confirms and reinforces that a Common Law duty of confidence applies to everyone working for or with the HSC and aims to inform all staff working within the PHA of the personal role they must play in the correct, appropriate and legitimate sharing of information, and what measures they must take to protect that information when it is in their charge.

This policy should be read by staff in conjunction with all Information Governance and ICT Security policies available on the PHA Intranet, as well as mandatory Information Governance eLearning training on the HSC Leadership Centre website. This policy should also be read in conjunction with the PHA privacy notices which can be found on the PHA Intranet.

This policy should be read alongside the PHA's Facilities Management Policies for each of the locations, which deal with physical security of the PHA's premises and give important guidance in this respect.

The policy has been written in line with current legislation and guidance on data protection, with particular reference to the then Department of Health, Social Services and Public Safety guidance document "Code of Practice on Protecting the Confidentiality of Service User Information" (January 2012). Reference is also made to the Data Protection Act 2018, GDPR and the revised Principles set out in Caldicott 2. This policy has been reviewed to reflect the additional Caldicott Principle "*The duty to share information can be as important as the duty to protect patient confidentiality*". Whilst not binding in the context of Northern Ireland, HSC has adopted these principles in spirit and they remain at the heart of all related policy developments.

1.3 Governing Principles

The following governing principles are at the heart of this policy document, and should be viewed as the defining principles when handling personal data.

1 The use to which Personal Information is to be put within or from an organisation should be clearly defined, justified and regularly reviewed.

2 Personal data items should not be included in transfers of information within or between organisations unless it is absolutely necessary, there is a robust business need and sufficient security measures employed to protect the transfer.

3 Only the minimum amount of identifiable information should be transferred or be accessible as is necessary for any given, specified and approved function or purpose.

4 Only those individuals who need access to personal information should have access to it, and limited to what they need to see for their particular business need.

5 Managers and 'Information Asset Owners' should take such actions as are necessary on an on-going basis to ensure that all staff are made fully aware of their contractual and legal responsibilities and obligations to respect and protect individuals' personal information from unauthorised use, disclosure, loss or destruction.

6 Every use to which personal data is put should be lawful and comply with all relevant applicable guidance.

7 No personal information should be transferred within or between organisations unless adequate, robust and approved security mechanisms are in place – see 2 above.

8 When collecting personal data from data subjects, PHA should inform the subject as to the proposed use or uses to which the data will be put, as well as who it is to be shared with, how it will be secured and how long it will be retained.

9 Personal Information will, when no longer required, be permanently and verifiably destroyed.

This policy also takes cognisance of the following GDPR principles:-

1. Transparency, fairness and lawfulness in the handling and use of personal data.
2. Limiting the processing of personal data to specified, explicit and legitimate purposes.
3. Minimising the collection and storage of personal data.
4. Ensuring accuracy of personal data and enabling it to be erased or rectified.
5. Limiting the storage of personal data.
6. Ensuring security, integrity and confidentiality of personal data.

The above principles should also be read in conjunction with the Individual's Rights under GDPR, which have been summarized in Appendix 6.

Compliance with this policy will ensure:-

- That the data collection is lawful and complies with the Data Protection Act 2018, GDPR and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- That data access is restricted to those with legitimate need to view the data.
- That all records and systems, electronic and manual, are secured and that all information held is a minimum data set, is collected and processed for specific purposes, is held only as long as is necessary for the purpose for which it was collected, is processed fairly and lawfully and is disposed of in a way which continues to protect confidentiality.
- That personal information is shared with those staff who have a legitimate relationship with the service user, are involved in the management and/or delivery of Health and Social Care Services or are regulated and registered Health and Social Care Professionals.

1.4 Definitions

"Personal Data" - The term "personal information" applies to personal data/ information, as is defined in law, about living individuals held by or for Health and Social Care organisations, agents or staff. Personal data is data which relates to a living individual who can be identified from those data.

This definition covers the obvious such as medical and staff records in addition to personal 'non-health' information such as a patient or client's name and address or details of his or her financial or domestic circumstances. It relates to both computerised and manual records and can be held in different formats, and include, for example, CCTV images microfiche, audio recording or still photographic images.

"Sensitive Personal Data" - Some "personal data" is classed as "sensitive personal data" by the Data Protection Act and additional safeguards and regulation is afforded to this type of information. This information can only be processed under certain defined circumstances.

'Personal data' becomes 'sensitive personal data' if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health;
- sexual orientation;
- commission of offences or alleged offences.

If you process information containing one or more of the types of information described above and have any queries relating to the extent of its use, transfer or permanent destruction, you may seek advice from the Senior Operations Manager (Delivery).

'Data Controller' - For the purpose of this document the Public Health Agency (PHA) is the "Data Controller" and, therefore, the organisation and its employees are subject to, and required to comply with, the principles set out in the Data Protection Act 2018 and the GDPR.

The Ministry of Justice defines the 'Data Controller' as, "*a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed*".

'Data Processor' - The Ministry of Justice defines the 'Data Processor', in relation to personal data, as any person (other than an employee of the data controller) who processes the data on behalf of the "data controller".

These definitions are also consistent with GDPR.

In relation to the PHA, this definition would define, for example, The Business Services Organisation, as a PHA data processor, in so far as the BSO processes information or carries out certain functions on behalf of the PHA.

In a legal context the PHA "owns" the "personal data" it "controls" and is responsible for ensuring compliance with the principles set out in the Data Protection Act 2018 and GDPR.

This extends to ensuring that adequate safeguards, that are at the very least equal to those employed by the PHA, are implemented and operated by a Data Processor to protect and comply with the Principles of the Data Protection Act when carrying out processing of personal information on our behalf.

1.5 Further Information

Further information regarding any aspect of data protection and use of personal information can be found on the Information Commissioner's Office website: https://ico.org.uk.

The PHA Senior Operations Manager (Delivery) will also be able to provide information about this policy.

2.0 BASIC PRINCIPLES

2.1 Every person, irrespective of Nationality, whose information is held by the PHA is afforded certain rights under the United Kingdom Data Protection Act 2018 and GDPR. The PHA is legally obliged to respect and maintain these rights in both practice and policy.

2.2 All PHA staff are legally bound by a Common Law duty of confidence to maintain confidentiality of information and abide by the principles of the Data Protection Act 2018 and GDPR.

2.3 Information provided in confidence may not be used for a purpose other than that for which it was collected or be passed to anyone else without the consent of the provider of the information (Data Subject). If occasion arises where it is proposed that personal information be used for another purpose, then expert opinion should be sought before any additional processing takes place.

2.4 Patients, clients and staff should, where it is reasonable and practicable to do so, be informed in advance of the uses to which their information may be put. (i.e. via PHA privacy notices).

2.5 Patients and clients' right to refuse or withdraw the use of their information must be respected (except in exempted circumstances where this is required by law).

2.6 The PHA is required to comply with all legislation and guidance relating to the protection and use of personal information.

2.7 Access to, and release of personal information will be strictly controlled; where possible anonymised and aggregate information will be used. Only the minimum data required will be processed by the PHA.

2.8 Personal information will be held only for as long as it is required for the purpose for which it was collected. It will be disposed of in a manner that continues to protect confidentiality. Patients, Clients and Staff should be informed at the outset regarding the period that their information will be retained.

2.9 Individuals have a right to complain to the ICO if they have concerns regarding the handling of their personal or sensitive information.

2.10 Contractors with access to personal information held by, or on behalf of, the PHA are required to comply with this policy and have in place their own complementary policies and procedures that will provide the same or greater protection to information processed on behalf of the PHA (see 1.3). The PHA will require that Contractors or Agents acting at the direction of the PHA provide assurances and evidence of this requirement. Where it is deemed necessary, the PHA will require Contractors or Agents to implement certain organisational and/or technical measures to enhance their existing information security measures. Contractors or Agents will also be expected to follow PHA good practice developments in information security, and amend their own processes to meet PHA expectations.

3.0 PROTECTION AND USE OF INFORMATION

3.1 Uses and restrictions

3.1.1 Patients, clients and staff should be advised in advance of the uses to which the information they provide may be put. This may be verbally, in written form on standard documentation used to collect information, or on literature on protection and use of personal information designed specifically for this purpose. These are known as ‘Privacy Notices’.

3.1.2 Personal information may *in appropriate circumstances* * be used for:

- The delivery of personal care and treatment, including needs assessment and Service Planning.
- For assuring, improving or auditing the quality of care and treatment delivered by HSC.
- To monitor and protect public health including the prevention, detection and control of disease.
- To co-ordinate HSC care with that of other associated agencies.
- For effective Health and Social Care administration.
- Teaching, training and education of Staff.
- In statistical analysis and/or Health and Social Care research.
- Staff Administration and records including pay, superannuation, work management and discipline.
- Accounting and Auditing including the provision of accounting and related services, the provision of an Audit where such an audit is required by statute.
- Crime prevention and prosecution of offenders.
- The administration of licensing or maintenance of official registers.
- Benefits, grants and loans administration.
- Investigation of complaints.
- Defending legal challenge.
- Auditing of Bodies in receipt of monies from the HSC.

*** Note**: This list of possible uses is not exhaustive. If you are unsure whether or not a particular use is covered here, advice should be sought from the PHA Senior Operations Manager (Delivery).

3.1.3 Sometimes, personal information is required by statute or court order and the PHA will be obliged to release the information in these circumstances.

3.1.4 Release of information necessary for the protection of the public and tackling serious crime is covered by the "Code of Practice on Protecting the Confidentiality of Service User Information" (January 2012) which should be studied in conjunction with this policy.

3.1.5 The PHA will not and does not permit personal details to be released or sold on for fundraising or commercial marketing purposes.

3.1.6 The PHA does not permit external Agents or Contractors to pass on information to third parties unless the purpose is legitimate and the PHA has agreed to that sharing in writing via a Data Access Agreement or Memorandum of Understanding.

3.1.7 The PHA is obliged by law to comply with requests from the Comptroller and Auditor General Northern Ireland to provide information in an electronic format relating to PHA staff for the purpose of Data Matching exercises conducted under the National Fraud Initiative. These powers are based on amendments to the Audit and Accountability Order (Northern Ireland) 2003, at Articles 4A and 4G respectively.

3.2 Collection, Retention and Disposal of Information

3.2.1 Data subjects will be advised of the uses to which their information may be put. This should take the form of information to patients and clients as laid out in the then DHSSPS "Code of Practice on Protecting the Confidentiality of Service User Information" (January 2012). They will also be advised on request of the rights of access which apply to certain records under the Data Protection Act 2018 and GDPR.

3.2.2 Information sharing between HSC bodies may require a signed Data Access Agreement between the parties. It is recommended that such an agreement is in place for those information flows regularly shared, for example, between the PHA and their Providers. A sample Data Access Agreement is included (Appendix 1).

3.2.3 Information sharing between HSC bodies and non-HSC bodies must also be covered by a Data Access Agreement.

3.2.4 Patients or Clients who consider withholding or restricting transfer of information should be advised that such restriction could possibly have an adverse impact on their care or treatment as the sharing of personal information between HSC professionals is critical to ensuring that the highest level of service is afforded to the individual. Legal or statutory requirements should also be explained. HSC staff should ensure that these discussions are handled with sensitivity and care and that the opinion of the individual is respected when making decisions about the use to which their information is to be put.

3.2.5 Only the minimum set of data should be collected, sufficient to the task.

3.2.6 Computerised personal information will be held on systems that are at the very least password protected and comply with the PHA ICT security policies and to which access is restricted to authorised personnel. Guidance on use of passwords is laid out in the PHAs ICT Security Policy. Any unauthorised access to restricted information must be brought to the attention of a senior officer immediately and the Senior Operations Manager (Delivery) must be informed at the earliest opportunity.

3.2.7 Removable media such as PHA approved ‘SafeStick’ USB devices, laptops and tablet devices must have encryption software installed to protect against unauthorised access to sensitive information

in the event of a loss or theft of that equipment. It is not permitted to store or transfer sensitive information, either corporate or personal, on media that is not encrypted, such as personal laptops, tablet devices or ‘SafeStick’ USB devices.

For security purposes each electronic or physical set of data is assigned an ‘information asset owner’. The IAO is responsible for:-

- Identifying all the data within their area of responsibility;
- Specifying how the data can be used;
- Agreeing who can access the data and what type of access each user is allowed. (See Appendix 1 addendum for PHA ‘Data Access Agreement Form’).
- Determining the classification or sensitivity level(s) of the data;
- Periodically reviewing that classification;
- Ensuring and approving appropriate security protection for the data, e.g. encryption software
- Ensuring compliance with security controls;
- Ensuring compliance, where necessary, with the Data Protection Act 2018, GDPR and any other relevant legislation covering personal or medical data;
- Ensuring all staff that they are responsible for and aware of their responsibilities and have access to policies and specialist advice when required.

Data classed as ‘sensitive’ within one system should maintain at least the same sensitivity level across all systems.

Access rights given to users should be consistent across all areas. Particular attention should be paid to data being downloaded to a computer. Corporately sensitive information often ceases to be sensitive after a period of time, for example, when the information has been made public.

This should be taken into account, as over-classification can lead to unnecessary expense.

Please note: As a general statement, it is not permitted for PHA personal data or PHA business information to be held on unencrypted desktop or laptop computers. Such information should be held on a dedicated records management system, a dedicated server or at a sufficiently secure location to mitigate against the risk of a loss or theft of that equipment and to ensure there are regular backups of that data to maintain business continuity. It is recognised that business needs will occasionally dictate that sensitive information is held on laptops or desktops. Staff should seek advice from the Senior Operations Manager (Delivery) to ensure adequate alternative safeguards are in place on these occasions.

3.2.8 Manual personal information will be held securely, for example in locked filing cabinets, and access restricted to authorised staff. Access will be granted at the direction of the Information Asset Owner or designated deputy (see 3.2.7)

3.2.9 Staff should operate a clear desk policy whereby personal (or business sensitive) information is not left in clear view of others (see PHA Clear Desk Policy).

3.2.10 Information will be retained only for as long as the purpose/s require(s) it, bearing in mind legal timescales for retention of particular records (Appendix 2). Individual departments within the PHA are required to be familiar and comply with the timescales under which the personal information they hold is governed. Reference should be made to the then DHSSPS document “Good Management Good Records” and the PHA “Records Management Policy” and “Retention and Disposal Schedule”. These can be found on the PHA Connect site policy section under Information Governance.

3.2.11 Methods used for disposal of confidential information must continue to protect confidentiality. Paper information should be shredded by means of a 'cross cut' shredder. It is not permitted to shred sensitive information by means of a 'strip' shredder as this method is no longer considered secure.

All redundant, faulty or obsolete PHA removable storage media, such as 'SafeStick' USB devices or external hard drives which did or which may have contained sensitive or valuable information during their life cycle, should be returned to the BSO Information Security Team (ITS) for complete and verifiable destruction rendering them unusable. An INFRA call should be logged to facilitate this type of equipment disposal. Officers responsible for the formal disposal of media should ensure that a disposal certificate is sought from any contractor employed to carry out this task. Further information on this area can be found in the PHA Waste Management Policy.

3.3 Processing and Presentation

3.3.1 Staff who are authorised to do so will process and present information in line with uses and restrictions set out in 3.1.

3.3.2 Information will be presented in an aggregate, anonymised form where disclosure of an individual's information would not be authorised for the purpose. Anonymisation does not, in itself, remove the duty of confidence in relation to the information. Confidentiality must still be protected.

3.3.3 With increasing usage of geographical information mapping tools (GIS) it is important to emphasise that, within the PHA, mapping systems are utilised only by trained staff who are fully aware of their personal responsibilities in protecting individual information from disclosure, both in its raw form and in any way in which it is potentially represented.

3.3.4 To allow the sharing of personal identifiable data within the terms of the Data Protection Act 2018 and GDPR, it is essential, when information is being gathered, that the purpose or purposes to which that information is to be used is clearly defined and understood by the data subject and that they agree to the proposed usage.

If you have captured this consent, sharing is legitimate within the terms and conditions of use to which the subject agreed. Any secondary use of patient level data should be considered in conjunction with advice from the PHA Senior Operations Manager (Delivery) in conjunction with the third party from which the information was received. In many cases, this will involve Trust providers' input.

3.3.5 **Information labelling and handling**.
Sensitive information should be labelled appropriately and output from systems handling such data should carry an appropriate classification label (in the output). The marking should reflect the classification of the most sensitive data in the output. Output includes all types of storage media and file transfers.

The document "Code of Practice on Protecting the Confidentiality of Service User Information" was issued by the Department of Health in 2012. Care should be taken to meet its requirements. This document can be found at the following web address:

https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information.

3.4 Disclosure

3.4.1 Disclosure of personal information will be on a strictly “need to know” basis in accordance with the uses detailed in 3.1 and, where necessary, in consultation with the Information Asset Owner

3.4.2 Information disclosed will be the minimum dataset, sufficient to carry out the task.

3.4.3 All requests made to the PHA by an individual, other than from a member of PHA staff, seeking access to their own personal information should be forwarded to the Senior Operations Manager (Delivery) at Tower Hill who will process the request in accordance with relevant statutory obligations.

3.4.4 Where information has been sought for research purposes by external organisations/individuals, a Data Access application should be issued and returned before an informed decision is taken on appropriateness of disclosure (Appendix 3).

3.4.5 For some guidance in relation to the risks associated with information requests, refer to the Department’s revised “Code of Practice on Protecting the Confidentiality of Service User Information” (January 2012).

3.4.6 In line with guidance laid down in the PHA’s ICT Security Policy and various protocols operating within the PHA, disclosure of any information must be via media appropriate to the sensitivity of the information concerned. Security measures such as passwords and encryption must be employed when transferring or storing personal (or corporately sensitive data) and that transfer or storage must be authorised by the department’s nominated Information Asset Owner. You should refer to the Information Governance Leaflets titled ‘Information Transfers: Your Options’ and ‘Information Security Leaflet’ for advice.

Further advice can be sought from the Senior Operations Manager (Delivery) or the Business Services Organisations Information Security Department (BSO ITS).

3.5 Data Access Requests

Data subjects (individuals whose information we hold) have the right to see or request a copy of data which is held about them, whether this be computerised or manual. All requests for access to personal information must be received in writing. The procedures for dealing with such requests are laid out at Appendix 4. Further advice may be sought through the Senior Operations Manager (Delivery).

3.6 Information for Statistics and Research

The sharing of PHA information for statistics and research purposes is governed primarily by the principles and schedules of the Data Protection Act 2018, GDPR and other complimentary Legislation and Regulatory Codes of Practice. The Body / Organisation requesting information is required to complete an 'Application for Access to Personal Level Data for Research Purposes' (Appendix 3) which must be submitted to the PHA for consideration. In the event that the PHA approves a disclosure of patient level data, a Data Access Agreement (Appendix 1 addendum) would be drafted to cover the disclosure and describe the use and extent of the disclosure. Note: Using information for research purposes is addressed within the Data Protection Act 2018. However, strict guidelines will apply and appropriate safeguards must be present in order for data to be used for research purposes within the strict definitions provided within the Act. Further advice may be sought from the Senior Operations Manager (Delivery) or PHA Personal Data Guardian.

3.7 Human Resources Records

Personal information is collected for recruitment purposes, for salaries and wages, for maintenance of the employment relationship between the PHA and its staff and to ensure that the PHA complies with its HR policies and procedures.

HR policies are available on the PHAs Connect site. It is important to recognise that any staff information held by managers (manual or electronic) should be afforded the highest levels of privacy and security. It should be noted that rights afforded to the individual under the Data Protection Act 2018 and GDPR extend to employees of the PHA and these rights are not lessened by virtue of the employer / employee relationship.

(Note: The PHA is a Public Authority as defined by the Freedom of Information Act 2000. In certain circumstances, information relating to employees public role within the PHA may be disclosed, for example, on receipt of a Freedom of Information request.)

3.8 Audit Records

The PHA is required to provide access to all its records to Internal Audit. This access extends to all records, documents and correspondence relating to any financial or other relevant transaction, or function or activity conducted by the PHA or its Officers and includes documents of a confidential nature. This disclosure of information is covered by the PHA's Data Protection registration with the Information Commissioner and Internal Auditors are contractually bound to maintain the security and confidentiality of all records in their care as with all personal information held at PHA level.

Further to this, the Comptroller & Auditor General under powers conferred to his Office through the introduction of the 'Audit and Accountability (Northern Ireland) Order 2003' will periodically require disclosure of information from the HSC when conducting Data Matching Exercises under the National Fraud Initiative. It should be noted that the HSC is legally bound to comply with any request for access to information held on both employees and contractors. Release of such information does not require the consent of the individuals concerned under the Data Protection Act 2018 and GDPR. Staff will be notified prior to any disclosure and additional information can be sought at that time from the PHA Senior Operations Manager (Delivery).

3.9 Responsibilities of Staff and Contractors

3.9.1 All staff are bound contractually to protect the confidentiality of information to which they have access in the course of their employment.

3.9.2 Provision currently exists in contracts between the PHA and its Providers to maintain confidentiality of information that is utilised in any dealings arising from the operation of the contract. Providers should ensure that any information disclosed to the PHA is anonymised where possible. Where identification of individuals is necessary, Providers should ensure that appropriate consent of data subjects is in place for the purpose of disclosure and that disclosure is in line with the provisions of all relevant legislation and applicable guidance. Providers should describe any conditions which are attached to the data at the time of transfer, such as retention and disposal timescales.

3.9.3 Comprehensive confidentiality clauses are currently written into contracts between the PHA and computer companies/agencies and general maintenance contractors which refer directly to the protection of personal data and confidentiality. All contractors have a responsibility under this policy and existing legislation to protect the information to which they have access under the terms of their contract.

3.9.4 Protocols, such as those for faxing information and operation of ‘safe haven’ addresses and associated contact persons, are currently shared with those Providers/contractors to whom they may apply.

3.10 Out of the Office

It is PHA policy that patient/client-identifiable information remains on-site where possible. The PHA expects that no patient, client or employee identifiable information will be removed from the building without the approval of a sufficiently authorised officer, normally the Information Asset Owner or Assistant Director level or above. Information Security measures such as passwords and encryption software should be present on any removable media device, such as a laptop, external hard drive or PHA approved and issued 'SafeStick' USB device, before any decision to allow information to leave the premises is taken. Reference should be made to PHA ICT Security Policy.

Requests for remote internet access can be made by completing the 'Secure Remote Access Application Form' which can be found on the Information Governance Section of the PHA Connect site. This form must be signed off at Assistant Director Level before it is considered by the Senior Operations Manager (Delivery) or Deputy.

3.11 Breaches of policy

3.11.1 All staff, contractors and agents are reminded that they are bound by a Common Law Duty of Confidence in the protection and use of personal patient, client and staff information. All staff, contractors and agents should be aware of and abide by the contents of this policy.

3.11.2 The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO within 72 hours. **Any suspected breach of this Policy must be reported to the Senior Operations Manager (Delivery) immediately.**

The incident can then be assessed and appropriate immediate and remedial corrective action taken to contain the breach. (Please refer to PHA Data Breach Response Policy).

4.0 PHA RESPONSIBILITIES

4.1 Management Arrangements

4.1.1 The PHA has approved this policy document in recognition of its responsibilities in relation to the protection and use of personal information as governed by the Data Protection Act 2018 and GDPR.

4.1.2 The PHA requires that Management make appropriate arrangements to ensure communication of this policy to all levels of staff within the organisation and ensure that staff receive and attend training courses relating to this particular subject.

4.1.3 Any queries arising in relation to this policy should be directed to the Senior Operations Manager (Delivery).

4.2 Resources

4.2.1 The PHA will consider the use of resources in developing materials to inform patients, clients and staff of the uses to which their information will be put and to their rights of access where appropriate.

4.2.2 Training to communicate the responsibilities laid out in this and associated policy documents and practical measures that can be taken to comply with the contents will be provided for all PHA staff in formats that meet the identified need with emphasis on e-learning packages.

4.2.3 Practical guidance for compliance with this policy and the ICT Security Policy will be provided for all staff. This information will also be provided in hardcopy, through the PHA Connect site and through e-learning packages accessible via staff computers.

4.2.4 It is envisaged that all new staff will be informed of their responsibilities in relation to this policy and the ICT Security Policy as part of the PHA induction to the organisation. All Managers will be responsible for ensuring staff are familiar with both policies and are aware of their responsibilities in relation to their particular business activity.

4.2.5 Periodically, internal audit will review PHA arrangements for adequately protecting and appropriate usage of personal information.

4.2.6 The Senior Operations Manager (Delivery) will make arrangements for periodic 'audits' of the main PHA buildings to ensure that all staff are familiar with and abiding by the contents of the policy and its associated guidance. Reports on these audits will be prepared for consideration by the relevant directing committees of the PHA.

4.2.7 Contractors will be made aware of the contents of this policy and their associated responsibilities through the HSC standard contract clauses.

4.3 Ensuring Adherence

4.3.1 Through effective communication, the PHA requires that staff act responsibly and within the confines of this policy document. However, breaches will be dealt with as serious matters and the PHA will not hesitate in exercising its rights in such situations.

4.3.2 Contractors working with or on behalf of the PHA will be informed that they too are bound by the principles laid down in this policy and the relevant clauses included in all contracts.

4.4 Equality and Human Rights Screening

4.4.1 This policy has been screened for equality implications as required by Section 75, Schedule 9, of the Northern Ireland Act, 1998.

Equality Commission for Northern Ireland Guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be devoted to them.

4.4.2 Using the Equality Commission's screening criteria, no significant equality implications have been identified. This policy will therefore not be subject to an equality impact assessment.

4.4.3 This policy has been considered under the terms of the Human Rights Act 1998 and was deemed to be compatible with the European Convention Rights contained in that Act.

4.4.4 This policy has been included in the PHA's Register of Screening Documentation and maintained for inspection whilst it remains in force.

4.4.5 This document can be made available on request in alternative formats and in other languages to meet the needs of those who are not fluent in English.

4.5 Review of policy

This policy will be periodically reviewed and updated to ensure that it is in line with current guidance and legislation relating to the protection and use of patient and client information.

Appendix 1

PHA DATA ACCESS AGREEMENT FORM (DAA)

The PHAs 'Data Access Agreement' pro-forma is provided as a separate file and can be accessed on the PHA Connect site under the Information Governance Section – link.

Appendix 2

Retention of Records

The retention and disposal of PHA records must be in line with both the PHA Records Management Policy and the corresponding Retention and Disposal Schedule. The Retention and Disposal Schedule is based on the then DHSSPS publication 'Good Management, Good Records' and outlines minimum retention periods for records created in the PHA. The Schedule also details the final action for PHA records by identifying those which need to be transferred to the Public Record Office for Northern Ireland (PRONI) and those which can be destroyed once they have been retained for the sufficient period of time.

The following link will take you to the Good Management, Good Records facility on the DOH website - link.

Appendix 3

APPLICATION FOR ACCESS TO PERSONAL LEVEL DATA FOR RESEARCH PURPOSES

1. Personal Details – Researcher / Planner

Surname :_____

Forenames :_____

Postal Address :_____

_____

_____

Postcode:_____

Organisation :_____

Telephone No. :_____

Fax No. :_____

Email :_____

2. Project Details

Title of Project :_____

_____

Project purpose:_____

/ background _____

_____

_____

_____

_____

_____

_____

Proposed Start Date : _____

Duration : _____

3. Approval sought by the Researcher / Planner

Identify organisations or individuals from which assurances of co-operation will be required and whether these assurances have yet been given.

Name of individual/organisation and contact name	**Co-operation confirmed (Y/N)**

Has this research been cleared by the Ethical Committee (where appropriate): _____

(*copy of authorisation to be attached to this application)*

Terms and Conditions of Support

The following are the Terms and Conditions under which the Public Health Agency (PHA) will consider supporting the proposed research:

4. GENERAL CONDITIONS

4.1 The Applicant will acknowledge the support of the PHA in any final report.

4.2 The Applicant will provide the PHA with an opportunity to contribute to the design of the research.

4.3 The Applicant will provide the PHA with a presentation of the findings of the research if requested to do so.

4.4 The Applicant will comply with all Data Protection requirements and will exercise proper safeguards to prevent any breach of confidentiality and/or privacy. Any disclosed results of the research shall not be able to identify an individual without that individual's written consent.

4.5 Data made available by the PHA to the Applicant is done so in confidence solely for the purpose of the above research project.

4.6 Data made available by PHA to the Applicant directly will not be divulged to any individual not associated with the research.

4.7 When the research project is concluded, all personal data will be entirely destroyed.

4.8 The Applicant will provide the PHA with a pre-publication draft of any report generated from the research prior to publication.

4.9 The Applicant will pay for any reasonable costs incurred by the PHA in supporting the research, including costs incurred by other organisations.

5. AGREEMENT (To be completed by the Researcher / Planner)

I agree to the terms and conditions laid out in this document.

Signed
Project Leader: _____
Organisation: _____
Date: _____

6. Declaration of Data Protection Co-ordinator and Data Custodian

I declare that the Public Health Agency's involvement in the above research complies with the Data Protection Act and that all notification requirements have been completed.

Signed: _____ (Data Guardian)
Date: _____

Signed: _____
(Senior Operations Manager (Delivery))
Date: _____

6.1 Chief Executive PHA (or Designated Deputy)

Signed: _____ (Chief Executive/Deputy)
Date: _____

Appendix 4

Procedure for dealing with subject access requests

Sample Letter

PHA ADDRESS

Dear Sir / Madam

The Data Protection Act 2018 and GDPR give everyone the right to seek access to their own personal information.

To request access to Health and Social Care records held by the Public Health Agency (PHA), please complete the attached 'application form' (2 pages). A letter of application is also acceptable (e.g. from a Solicitors office) but it should provide us with all necessary information to allow us to search for any relevant records.

Please include as much detail as possible about the records you are seeking e.g. type, location or any reference number you may have received from the PHA during previous correspondence.

The completed Application Form or letter of application should be returned along with;

a) A valid form of identification (e.g. driving licence, birth certificate, ID card, passport – originals will be returned).
b) If the application is from someone other than the subject of the information, signed consent from the data subject.

I am required to inform you that the one month allowed under DPA and GDPR to process your request will not commence until we receive all necessary documentation as indicated above.

If you have any queries about completing this Application Form, or about our procedures for processing such requests, please do not hesitate to contact me at the address provided.

Should you wish to complain, please contact ....

Yours Sincerely

_____

Application for access to personal Health and Social Care records

**(A valid form of identification should accompany all requests;
see form for details of any documentation required to validate your application)**

PART A

Your details (person to whom the information relates)

Surname Forenames

Date of Birth Other identifying Information

Address

Tel / Contact Number

If the details provided above are different from those that we may hold about you, please provide us with the following information

Previous Surname (1)_____ (2) _____

Previous Address (1)_____ (2) _____

Applicable dates _____

To help us identify the records you are seeking, please indicate what type of record you believe we may hold (e.g. Complaints records, Social Services records, Health records)

PART B I require access to the records in the following format: Please Tick

I only wish to view my records ☐

Printout of records held on computer systems ☐

A copy of Social Services Records (paper records only) ☐

A copy of Health Care Records (paper records) and/or copies Of X-Ray film ☐

Part C Applicant's details (if not the person to whom the data relates)
If you are applying to see records that are not your own, please provide details:

What is your relationship to the person to which the information relates:

Your surname Your Forenames

Your Address

Your Tel / Contact Number
(this is the address to which a reply or other correspondence will be sent, unless otherwise stated)

Please indicate below by ticking relevant box or deleting as appropriate

I have been asked to act on behalf of the person whose information is being sought and their written permission is included (Part E below) ☐

I am acting in parental capacity as the person whose information is being sought is under 16 years of age and: is incapable of understanding the request* OR has consented to my making this request*
(*delete as appropriate) ☐

The person is over the age of 16, however is incapable of understanding the request and I therefore act as his/her personal representative ☐

The person is deceased and I am the next of kin ☐

The person is deceased and I am his/her personal representative and attach legal documents confirming my position ☐

PART D To be completed by the person requesting access to records

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to request access to the records detailed above.

_____ _____ _____/_____/_____
Print Name (capitals) Signed Date

PART E To be completed by the person to whom the information relates to authorise release of records to the individual named at **PARTC**

I hereby authorise the Public Health Agency to release the records detailed on this form to

_____representative named at **PART C**)

Signed_____ Date_____
(person to whom information relates)

Appendix 5

DATA PROTECTION PRINCIPLES, 2018 ACT

The principles of protection of personal data are contained within the Data Protection Act 2018. These impose specific requirements on PHA staff when handling Personal Data.

First Principle: Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless:

- At least one of the conditions in Schedule 2 is met.
- In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

(NB: Health and Social Care data is, by nature, sensitive data and consequently requires grounds drawn from both schedules to justify processing. In legal terms, if data subject consent, explicit or otherwise, is lacking, then performance of functions under enactment of government functions or performance of a medical function may suffice).

Second Principle: Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Third Principle: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle: Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth Principle: Personal data shall be processed in accordance with the rights of the data subjects under this Act.

Seventh Principle: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

Eighth Principle: Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

More detailed information on the Data Protection Act 2018 can be obtained from the Senior Operations Manager (Delivery) or the Information Commissioner's website at https://ico.org.uk/.

This policy also takes cognisance of the following GDPR principles:-

1. Transparency, fairness and lawfulness in the handling and use of personal data.

2. Limiting the processing of personal data to specified, explicit and legitimate purposes.

3. Minimising the collection and storage of personal data.

4. Ensuring accuracy of personal data and enabling it to be erased or rectified.

5. Limiting the storage of personal data.

6. Ensuring security, integrity and confidentiality of personal data.

Appendix 6

Individual Rights under GDPR

The GDPR provides the following rights for individuals:

1. The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Organisations must provide individuals with information including: the purposes for processing personal data, the retention periods for that personal data and who it will be shared with. This is called 'privacy information'.

2. The right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

4. The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing.

The right is not absolute and only applies in certain circumstances.

5. The right to restrict processing

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, you are permitted to store the personal data, but not use it.

An individual can make a request for restriction verbally or in writing.

6. The right to data portability

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 hindrance to usability.

7. The right to object

Individuals have the right to object to:

processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

direct marketing (including profiling); and

processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling

The GDPR has provisions on:

automated individual decision-making (making a decision solely by automated means without any human involvement); and

profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Appendix 7

The Caldicott Principles (Best Practice)

The principles for dealing with patient-identifiable information are:

1) Justify the purpose(s). Every proposed use of transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed by an appropriate guardian.

2) Don't use personal confidential data unless it is absolutely necessary. Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3) Use the minimum necessary personal confidential data. Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4) Access to personal confidential data should be on a strict need to know basis. Only those individuals who need access to personal confidential data should have access and then only to the specific data items they need. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5) Everyone with access to personal confidential data should be aware of their responsibilities. Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6) Comply with the law. Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7) The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.