GIG CYMRU NHS WALES | Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

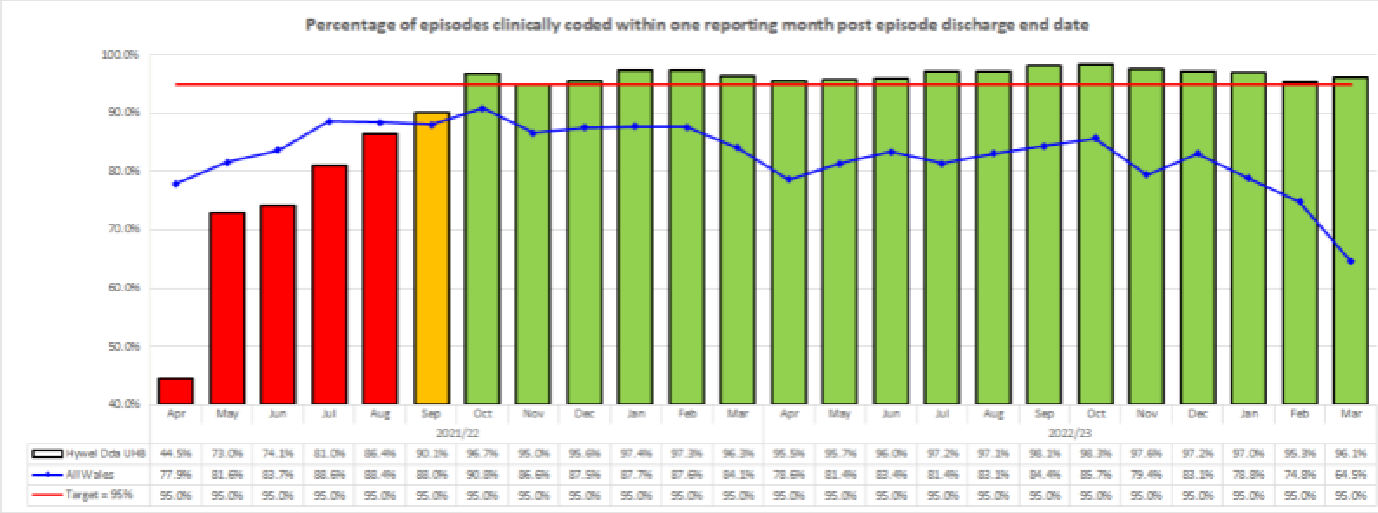
Enw yr Is-Bwyllgor: Name of Sub-Committee:	Information Governance Sub-Committee (IGSC)
Cadeirydd yr Is-Bwyllgor: Chair of Sub-Committee:	Huw Thomas, Executive Director of Finance
Cyfnod Adrodd: Reporting Period:	8 April 2023

Y Penderfyniadau a'r Materion a Ystyriodd yr Is-Bwyllgor:
Key Decisions and Matters Considered by the Sub-Committee:

Policies and Procedures:
The Sub-Committee received the following policies for approval.

- 191 – Health Records Management Strategy – approved to be passed to the Committee for approval
- 192 – Health Records Management Policy – approved to be passed to the Committee for approval

Clinical Coding Update
The Sub-Committee received a paper providing an update on the clinical coding position for the Health Board. Health Board performance has achieved the 95% target since October 2021, with latest performance for March 2023 provisionally at 96.1%.



	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Hywel Dda UHB	44.5%	73.0%	74.1%	81.0%	86.4%	90.1%	96.7%	95.0%	95.6%	97.4%	97.3%	96.3%	95.5%	95.7%	96.0%	97.2%	97.1%	98.1%	98.3%	97.6%	97.2%	97.0%	95.3%	96.1%
All Wales	77.9%	81.6%	83.7%	88.6%	88.4%	88.0%	90.8%	86.6%	87.5%	87.7%	87.6%	84.1%	78.6%	81.4%	83.4%	81.4%	83.1%	84.4%	85.7%	79.4%	83.1%	78.8%	74.8%	64.5%
Target = 95%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%

Hywel Dda University Health Board's (HDdUHB) Corporate and Medical Records Storage Assurance Report – Update
The Sub-Committee received an update on the current audit of storage facilities across the Health Board. The IG team has agreed, with the Withybush Senior Team, the audits to be undertaken week commencing 5 June and 12 June 2023 alongside a member of the corporate nursing team. Updates will be provided to the Sub-Committee once completed.

Information Commissioner Office (ICO) Notifications
Since April 2022, there have been five occurrences when a notification to the ICO has been required. The following table highlights the current notifications:

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total

Open	1	0	1	0	1	0	0	0	1	-	-	1	5
Closed	-	-	-	-	-	-	-	-	-	-	-	-	0
Total	1	0	1	0	1	0	0	0	0	0	0	0	5

All the above cases are still in progress and are awaiting responses from the Information Commissioners Office (ICO). For the financial year 2023/2024, **no** breaches have been reported to the ICO.

Welsh Information Governance Toolkit – Managed Practices

The Sub-Committee received an updated plan for assisting the Managed Practices in their compliance with Data Protection legislation and to work towards achieving a higher level of attainment in their IG Toolkit submissions, which are due for submission by 30 September 2023. The Sub-Committee was concerned with the increasing number of managed practices and the impact upon the information governance team resources to deliver the IG workplan. It was agreed that a new IG risk would be raised.

IG Annual Report (2022 – 2023)

A separate report has been prepared for presentation to the Committee meeting of the Sustainable Resources Committee.

Swine Flu Vaccination Records

The Sub-Committee received a paper on the destruction of Swine Flu Vaccinations Records (circa 2009). The Sub-Committee endorsed option 3 included within the paper, which is to destroy the records based on risk proportionate basis, in that these records should be considered as a patient record, and therefore is eligible to be destroyed after 8 years.

Cyber Security and Network and Information Systems (NIS) Directive Update

A separate report has been prepared for presentation to the In-Committee meeting of the Sustainable Resources Committee to provide an update on progress of Cyber Security.

Materion y Mae Angen Ystyriaeth neu Gymeradwyaeth Lefel y Pwyllgor Adnoddau Cynaliadwy:
Matters Requiring Sustainable Resources Committee Level Consideration or Approval:

Approval of the following policies:

- 191 – Health Records Management Strategy, attached at Appendix 1.
- 192 – Health Records Management Policy, attached at Appendix 2.

Approval of the following procedures, which have previously been agreed by the Sub-Committee:

- 1088 Information Rights Procedure, attached at Appendix 3.
- 773 Unauthorised Access to Patient Records - Reporting And Escalation Procedure, attached at Appendix 4.

Risgiau Allweddol a Materion Pryder:
Key Risks and Issues / Matters of Concern:

- The wider strategic issue of the storage of records and boxes within external storage companies.

Busnes Cynlluniedig yr Is-Bwyllgor ar Gyfer y Cyfnod Adrodd Nesaf:
Planned Sub-Committee Business for the Next Reporting Period:

Adrodd yn y Dyfodol:

Future Reporting:
• Information Asset Owners and Information Asset Mapping Update • Data Quality and Clinical Coding • Information Governance Risk Register • Information Governance Toolkit improvement plan • Update on Cyber Security / NISR • Caldicott Register to be returned to the IGSC meetings • Digital / IG Policies and Procedures
Dyddiad y Cyfarfod Nesaf: **Date of Next Meeting:**
8 August 2023

Health Records Management Strategy

Policy information

Policy number: 191

Classification: Corporate

Supersedes: Previous Version

Version number: 4

Date of Equality Impact Assessment:
09/05/2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:
Enter approval date
Date made active:
Enter date made active (completion by policy team)
Review date:
Enter review date (normally three years from approval date)

Summary of document:
This strategy addresses the principles and practice for managing health records within Hywel Dda University Health Board**.**

Scope:
This strategy has been written to provide an overarching framework of professional advice and guidance for all Hywel Dda University Health Board staff, to ensure compliance with all legal requirements for the maintenance, storage and provision and security of records. The strategy defines standards for improving the quality, availability and effectiveness of records management activities. This strategy applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

To be read in conjunction with:
[192] – Health Records Management Policy – opens in a new tab
[193] – Retention and Destruction of Records Policy – opens in a new tab
[249] – Access to Health Records Policy – opens in a new tab
[172] – Confidentiality Policy – opens in a new tab

[836] – All Wales Information Governance Policy – opens in a new tab
[837] – All Wales Information Security Policy – opens in a new tab
[347] – Corporate Records Management Policy – opens in a new tab

Patient information:

Owning group:
IGSC

Date signed off by owning group

Executive Director job title:
Director of Operations

Reviews and updates:
1 New policy September 2012
2 Full review 23.2.2016
3 DPA update 26.6.2018
4 Full review

Keywords
Health Records, Records Management

Glossary of terms
Records management - is that "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

A record - A health record is "one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of that individual". Anything that contains information that has been created or gathered as a result of any aspect of the work of NHS employees.

Data Protection Act 2018 - The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and replaces the Data Protection Act 1998.

Information Security - The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Public Records Act 1958 - The Public Records Act 1958 is an Act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom.

Contents

Introduction

This strategy addresses the principles and practice for managing health records within Hywel Dda University Health Board (HDUHB). The organisation uses a hybrid of computer and paper records to support patient processes and patient care and the strategy establishes how all patient records will be managed. Health Records management is about the proper content, control, security, storage and ultimate destruction of records. Records created and held by HDUHB as part of its functions, are public records under the Public Records Act 1958. The Public Records Act 1958 requires that there is a systematic and planned approach to the management of records within an organisation.

Effective management of healthcare services can only be achieved if there are appropriate health records management policies and processes in place. Health records management falls within the remit of the Health Records service. The aim of the health records service is to ensure that procedures are in place to bring together the health professional and accurate, relevant patient information/documentation at the correct time and place, to support patient care. Records management is a key component of the health records service and an expert professional field. The correct creation, management and maintenance of the health record provides the communication tool between the health professional and the patient.

The strategy details the aims, aspirations and targets of what we want to achieve with our health records management programmes and provides direction within the organisation. The Board, Executive Team, senior management and all who work for the organisation have responsibilities to ensure that information is handled appropriately and functions are performed in line with the required records management standards, ensuring the accuracy and availability of records for patient care.

The strategy will be updated as required to include future developments such as updated health records management guidance, to reflect technological changes such as the introduction of scanning services and the possible migration to an electronic patient record or changes in legislation.

This strategy is based on the requirements of the Records Management Code of Practice for Health and Social Care. This document covers management of all types of NHS health records throughout their lifecycle, from their creation and use, to their final disposal. This strategy should be read in conjunction with other HDUHB policies e.g. HDUHB Health Records Management Policy, Retention and Destruction Policy, Access to Health Records Policy etc and also the Data Protection Act.

Scope

This strategy has been written to provide an overarching framework of professional advice and guidance for all Hywel Dda University Health Board staff, to ensure compliance with all legal requirements for the maintenance, storage and provision and security of records. The strategy defines standards for improving the quality, availability and effectiveness of records management activities. The strategy clearly identifies all critical elements of effective records management and identifies key individuals within HDUHB and their obligation to ensure records are managed in accordance with legal requirements and both national and local standards.

This strategy relates to all clinical operational records held in any format by the HDUHB. Within the strategy the terms 'Health Record', 'Patient Record' and 'Case record' are synonymous and include:

- Records of patients treated by HDUHB including health and care records
- Records of private patients treated on NHS premises
- Records of patients treated on behalf of the NHS in the private healthcare sector

Health Records may be held in many formats, for example:

- Personal health records (electronic, microfilmed, scanned images & paper based)
- Theatre Registers and all other registers that may be kept
- X-ray and imaging reports, output and images
- Photographs, slides and any digital images
- Audio and video tapes, cassettes
- Digitised images/Digital Records (scanned)
- Emails
- Text messages (SMS)

This list is not exhaustive.

This strategy applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

Aim

The aim of the Health Records Management Strategy is to provide an overarching framework for current records management activities and initiatives, as well as any new ones recommended in the future. The Strategy will ensure there is:

- a systematic and planned approach to health records management covering health records from creation to disposal.
- efficiency and best value for money through improvements in the quality and flow of information, and greater co-ordination of health records and storage systems.
- compliance and delivery with statutory and legislative requirements.
- awareness of the importance of health records management and the need for responsibility and accountability at all levels.
- appropriate archiving of non-current health records.
- improve data quality to ensure accuracy and consistency.
- provide assurance around governance, confidentiality and data protection.

Objectives

The objectives of the strategy is to define an agreed approach for improving the quality, availability and effective use of records in the HDUHB and provide a strategic framework for all records management processes and procedures. This will enable overall coordination of all records management activities and ensure alignment with the HDUHB's business model. The key objectives associated with the strategy is improved patient safety and quality of care with the deliverable benefits being:

- the improved maintenance of the history of patient care and better communication and information sharing between care providers and patients
- greater efficiencies from the improved management of clinical functions
- reduced duplication of effort
- greater accountability and corporate governance
- reduction in litigation costs through improved patient safety and ability to defend against claims
- compliance with legislation and best practice record standards.

Responsibility and Accountability

There should be a clear chain of management, accountability and responsibility for all records created and utilised within the HHDUHB. The Chief Executive has overall accountability for ensuring that records management operates appropriately and a duty to make arrangements for the adequate resourcing and safekeeping of all HDUHB records. The Chief Executive may delegate responsibility for records management arrangements within the organisation to a designated Executive, who is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. The Medical Director has particular responsibilities for patient records as the Calidcott Guardian of the HDUHB.

The health records manager has strategic and operational accountability for the creation, retrieval, storage, archiving and disposal of all health records within the HDUHB. The HDUHB has in place a documented 191 - Health Records Management Policy and 193 - Retention and Destruction Policy – opens in a new tab - and detailed documented procedures, to support the life span of a health record from creation to disposal.

All staff should be aware of their individual responsibility and accountability in the creation, management, storage and access to all HDUHB records. More detailed information in regards specific HDUHB roles and responsibilities can be found in the 191 - Health Records Management Policy – opens in a new tab.

Standards of Records Management

The Health Records Management Strategy compromises of the following key elements.

Record Quality

The Health Records Management Strategy aims to provide assurance that policies and procedures are in place to ensure that the patient and health professional, together with accurate, relevant, reliable patient information and documentation are available at the correct time and place to support effective and safe patient care. HDUHB records should be accurate and complete, in order to facilitate audit and fulfil the HDUHB's responsibilities and protect its legal and other rights.

Records should show proof of their validity and authenticity so that any evidence derived from them is clearly credible and authoritative. Records should be retained securely and should only be shared or merged where appropriate. The 192 - Health Records Management Policy – opens in a new tab- and appendix of policies and procedures provide further detail specifically on standards for the management of health records. Health records are managed in accordance with the standards detailed in the introduction of this strategy.

Management

All health records are subject to the standards and legislation detailed in this strategy and the HDUHB is responsible for ensuring that health records are managed accordingly. Record-keeping systems should be easy to understand, clear, and efficient in terms of minimising staff time and optimising the use of space for storage. The 192 - Health Records Management Policy – opens in a new tab - details procedures for the storage, retrieval, archiving and disposal of each record type. This strategy is in accordance with the Welsh Records Management Code of Practice for Health and Social Care.

There should be a consistent approach to records management across the HDUHB, which should be in line with external guidance. The HDUHB is responsible for ensuring that adequate resources are made available to support effective records management, including making adequate provision for records growth and technological developments which enable records to be stored or transferred to other media. Investment in the move from paper to electronic records will become critical and will support improved patient care and service delivery not only within the health records service but across the entire HDUHB.

Security

The HDUHB provides systems which maintain appropriate confidentiality, security and integrity for all health records including their storage and use. Records must be kept securely to protect the confidentiality and authenticity of their contents and to provide further evidence of their validity in the event of a legal challenge. No person identifiable information should be stored, transferred or accessed unless absolutely necessary.

Health records in any format are highly confidential documents and the HDUHB is responsible for ensuring that adequate physical controls are put in place to ensure the security and confidentiality of all patient identifiable information, whether they are held manually (physically) or on computer (electronically). Other relevant policies and procedures are documented, including the 837 All Wales Information Security Policy – opens in a new tab - and they should be utilised in conjunction with local departmental procedures.

Access

Access is a key part of any records management strategy. Fast, efficient access to records unlocks the information and knowledge they contain. There should be clear and efficient access for employees and others who have a legitimate right of access to HDUHB records. Access to all patient identifiable information is on a strict need to know basis in accordance with the Caldicott principles, Data Protection Act 2018, General Data Protection Regulation, Information Governance Standards and various codes of professional conduct. Health Records Policies, including the 249 Access to Health Records Policy – opens in a new tab - and supporting procedures governing access to patient identifiable information all comply with and are in accordance with these principles.

The public has rights of access to all information held by the HDUHB, unless that information is covered by an exemption. Not only must records be maintained appropriately, when it is necessary to pass them to another user or stakeholder, care must also be taken to ensure that they are dispatched in a manner suitable to the content of the records. All managers are responsible for ensuring that there is an appropriate system for tracking and retrieving records when requested legitimately and that non-legitimate requests for records are declined.

Health records and associated clinical information are released to patients, their representatives and legal bodies in accordance with relevant and current legislation, including:

- Access to Health Records Act 1990
- Data Protection Act 2018
- General Data Protection Regulation (UK GDPR)

This list is not exhaustive.

The Health Records Manager is responsible for the processing and release of clinical information in accordance with the 249 Access to Health Records Policy – opens in a new tab - and documented procedures.

Retention and Disposal

Retention is the holding of records after their creation in readiness for operational use. It is a fundamental requirement that all the HDUHB records are retained for a minimum period for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the HDUHB's business and clinical functions. The Records Management Code of Practice for Health and Social Care establishes the minimum retention periods for a number of records and these requirements are reflected in the 193 Retention and Destruction Policy – opens in a new tab.

When considering how long to retain a record staff should first note any legal or HDUHB requirement. Records should be retained for the identified minimum requirements and storage in excess of the specified retention period is undesirable. During the retention period appropriate arrangements must be made for the safe storage and effective security of the record and considerations should be given to the storage medium (electronic or paper). Records no longer needed for operational or any other use should be destroyed. It is particularly important that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies and always through confidential processes.

Legislation

This strategy is based on current legal and statutory obligations and best practice and processes for records management. The Strategy also takes into account the recommendations and standards set by:

- Public Records Act 1958;
- Medical Reports Act 1988;
- The Computer Misuse Act 1990;
- Access to Health Records Act 1990;
- Data Protection Act 2018;
- Human Rights Act 2000;
- Freedom of Information Act
- Welsh Assembly Government (Ministerial Letters, Circulars and Policies);
- Caldicott: Principles into Practice;
- Information Sharing Protocols - Wales Accord on the Sharing of Personal Information
- Data accreditation and data quality

The strategy will be updated as required to include future developments such as updated health records management guidance, updates to statutory legislation, policies, protocols, Acts, etc and to reflect technological changes.

Risk Management and Patient Safety

Systems, policies, procedures and processes are in place to ensure that any risks to the record or the patient as a result of record issues, are identified, assessed and managed according to best practice.

Audit

This Health Records Management Strategy will be audited accordingly based on compliance against the aims, objectives and responsibilities outlined within the 192 - Health Records Management Policy – opens in a new tab.

Training

As the volume and complexity of clinical information increases, we demand the highest standards of performance in the way it is gathered, recorded, stored and transmitted. These requirements are set out in the Introduction of this strategy and throughout the document. Implementation of the strategy, within the HDUHB will put in place explicit guidance on legal and ethical responsibilities for all NHS staff involved with the creation, maintenance and ongoing management of health records. By utilising appropriately referenced publications, the Strategy will ensure compliance with legislation, nationally recognised standards and best practice.

Ongoing workforce education plays a major part in preparing NHS staff to deliver effective, high quality services. There are numerous reasons for providing education and training in information handling, including maintenance and improvement of services, respect to patients as well as the need to comply with legislation in respect of data collection, storage and use. Appropriate training will be given to all health records staff on the systems used to maintain records and these will meet local and national standards. The Health Records service is able to support awareness sessions or bespoke sessions as and when required to increase the awareness of individual staff responsibilities in regards records management. Self-learning modules are available to all staff through the HDUHB's intranet and ESR application.

GIG CYMRU NHS WALES | Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

Health Records Management Policy

Policy information

Policy number: 192

Classification: Corporate

Supersedes: Previous Version

Version number: 4

Date of Equality Impact Assessment:
17/04/2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:
Enter approval date
Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
This policy sets out best practice for the creation, utilisation, retention and destruction of health records within Hywel Dda University Health Board (HDUHB).

Scope:
This policy has been written to provide advice and guidance for all Hywel Dda University Health Board staff dealing with operational records management issues on a daily basis. The Policy highlights the standards that should be attained by all staff when utilising records from creation until final disposal. This policy applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

To be read in conjunction with:
[192] – Health Records Management Policy – opens in a new tab
[193] – Retention and Destruction of Records Policy – opens in a new tab
[249] – Access to Health Records Policy – opens in a new tab

[172] – Confidentiality Policy – opens in a new tab
[836] – All Wales Information Governance Policy – opens in a new tab
[837] – All Wales Information Security Policy – opens in a new tab
[347] – Corporate Records Management Policy – opens in a new tab

Patient information:

Owning group:
IGSC

Date signed off by owning group

Executive Director job title:
Director of Operations

Reviews and updates:
1 New policy September 2012
2 Full review 23.2.2016
3 DPA update 26.6.2018
4 Full review

Keywords
Health Records, Records Management

Glossary of terms
Records management - is that "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

A record - A health record is "one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of that individual". Anything that contains information that has been created or gathered as a result of any aspect of the work of NHS employees.

Data Protection Act 2018 - The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and replaces the Data Protection Act 1998.

Public Records Act 1958 - The Public Records Act 1958 is an Act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom.

Subject Access Request – Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'. Individuals can make SARs verbally or in writing, including via social media.

Data Protection Impact Assessment – Describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

Contents

Introduction

Hywel Dda University Health Board (HDUHB) will conduct its responsibilities for records management in accordance with relevant legislative requirements of the European Parliament, the United Kingdom and Welsh Government. HDUHB will also comply with any decisions or guidance issued by Welsh Government.

Health Records form an integral part of the clinical recollection of HDUHB, providing evidence of decisions, the rationale for decisions and supporting the HDDUB daily functions and operations. As contemporaneous records they form the basis for the organisations accountability for clinical care. Health records are also essential to protect the rights of patients, staff and members of the public who have dealings with the HDUHB. Health Records support consistency, continuity and efficiency and help the Board to deliver services to our patients in a consistent and equitable way.

Health Records management is about the proper content, control, security, storage and ultimate destruction of records. Records created and held by HDUHB as part of its functions, are public records under the Public Records Act 1958. The Public Records Act 1958 requires that there is a systematic and planned approach to the management of records within an organisation. Moving forward, the effectiveness, safety, care and efficient management of healthcare services, depends on the right information being available to the right people, at the right time. This can only be achieved if there are effective health records management policies and processes in place.

The Board, Executive Team, senior management and all who work for the organisation have responsibilities to ensure that information is handled appropriately and is not retained unnecessarily beyond its life cycle. We also have a responsibility to ensure the accuracy of records and to be able to identify and locate information that is critical for current decision making and available when required for patient care.

This document should be read in conjunction with other HDUHB policies e.g. HDUHB 191 Health Records Management Strategy, 193 - Retention and Destruction Policy, 249 - Access to Health Records Policy – all open in a new tab - etc and also the Data Protection Act.

Scope

This policy has been written to provide advice and guidance for all Hywel Dda University Health Board staff dealing with operational records management issues on a daily basis. The policy highlights the standards that should be attained by all staff when utilising records from creation until final disposal. This policy applies to all permanent, temporary or contracted staff employed by HDUHB (including Executive and Non – Executive Directors).

Aim

The aim of this Health Records Policy is to ensure that procedures are in place to bring together the health professionals and accurate, relevant and reliable patient documentation, at the correct time and place to support patient care. In achieving this aim, HDUHB employees should fulfil statutory and other legal requirements, ensuring patient safety and safe custody and confidentiality of patient information at all times.

The Health Records Management policy applies to all health records and personal information collated in relation to clinical activities and patient care. As the HDUHB utilises a hybrid of both paper and electronic records to support clinical processes this policy and the agreed standards of records management will fully apply to both formats. The policy sets out best practice for the creation, utilisation, retention and disposal of health records. It applies to all health records regardless of format, of all types and in all locations where they are used to:

- to support patient care and the continuity of care
- to support evidence based clinical practice
- to assist clinical and other types of audits
- to support improvements in clinical effectiveness through research and support archival functions by taking account of the historical importance of material and the needs of future research
- to support the day-to-day business which underpins the delivery of care
- to support sound administrative and managerial decision making as part of the knowledge base for the NHS services
- to support patient choice and control over treatment and services designed around patients
- to meet legal requirements including requests from patients under subject access provisions of the Data Protection Act

Objectives

The objective of this policy is to ensure that health records management is applied consistently across the HDUHB and draws on best practice, as well as ensuring that our services meet the legal, professional and individual responsibilities associated with record keeping. It is designed to provide the staff who create, hold and utilise the health record in the course of their duties with their obligations and expectations and help to increase the confidentiality, integrity and availability of the health record.

The policy relates to all health records which are created carrying out the HDUHB business and captured in any readable form, providing evidence of the patient care delivered. The policy provides all HDUHB staff with clear guidance and standards to attain on a daily basis and robust assurance that health records management systems are able to ensure that:

- **health records are available when needed** – from which the HDUHB is able to form a reconstruction of activities or events that have taken place
- **health records can be accessed** – health records and the information contained within them can be located and displayed in a way which is consistent with the records initial use and that the current version is identified where multiple volumes exist;
- **health records can be interpreted** – the context of the record can be interpreted; who created or added to the health record and when, during which business process, and how the health record is related to other health records
- **health records can be trusted** – the health record reliably represents the information that was actually used in or created by the business process, and the record integrity and authenticity can be demonstrated;
- **health records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the health record is needed, perhaps permanently despite changes of format;
- **health records are secure** – from unauthorised and inadvertent alteration and erasure. Access and disclosure are properly controlled and audit trails will track all use and changes to ensure that health records are held in a robust format;

- **health records are retained and disposed of appropriately** – using consistent documented retention and disposal procedures which include provision of appraisal and permanent preservation for health records with archival value;
- **staff are trained** – all staff within the organisation are made aware of their responsibilities for health record keeping and management.

Health Records Resource

Records are a valuable resource because of the information they contain. Information is only useful if it is correctly recorded in the first place, is regularly updated and is easily accessible when it is needed. Information is essential to the delivery of high quality healthcare and effective records management. The records and formats will include (but is not limited to):

- Records of patients treated by HDUHB including health and care records
- Records of private patients treated on NHS premises
- Records of patients treated on behalf of the NHS in the private healthcare sector
- Adult Service user records where there is integration with health services e.g. jointly held records

This list is not exhaustive.

A health record is everything (paper or electronic) that contains information which has been created or gathered as a result of any aspect of the delivery of patient care, including (but not limited to):

- Personal health records (electronic, microfilmed, scanned images & paper based)
- Theatre Registers and all other registers that may be kept
- X-ray and imaging reports, output and images
- Photographs, slides and any digital images
- Audio and video tapes, cassettes
- Digitised images/Digital Records (scanned)
- Emails
- Text messages (SMS)

This list is not exhaustive.

Roles and Responsibilities

All health and care employees are responsible for managing records appropriately. Health records management must provide a focus for all types of records, in any format to be managed from their creation to ultimate disposal. The health record management function must have clear responsibilities and accountability throughout the HDUHB.

Chief Executive

The Chief Executive has overall accountability and responsibility for ensuring that health record management operates correctly and legally within the HDUHB. The CEO may delegate responsibility for management and organisation of the health records services to the Caldicott Guardian or another Director who will be responsible for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

Caldicott Guardian/SIRO

The Caldicott Guardian/SIRO are responsible for protecting the confidentiality of service user information. The Caldicott Guardian/SIRO have strategic roles which involve representing and championing

information governance requirements and particular responsibility for reflecting patients' interest regarding the use of patient identifiable information.
The Caldicott Guardian has responsibility for:

- Ensuring the HDUHB is fulfilling all legal obligations in managing patients' health records
- Agreeing and reviewing internal protocols governing the protection and use of patient identifiable information by HDUHB staff
- Agreeing and reviewing protocols governing the disclosure of patient information across organisational boundaries e.g. with social services and other partner organisations, contributing to the local provision of care (WASPI)
- Developing the HDUHB security and confidentiality policies through the clinical and information governance frameworks
- Representing confidentiality requirements and issues to the HDUHB, advising on annual improvement plans and agreeing and presenting outcome reports

The SIRO is responsible for:

- Fostering a culture for protecting and using data
- Provides a focal point for managing information, risk and incidents
- Is concerned with the management of all information assets
- Acts as an advocate for information risk on the Board and provides written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk

Executive Directors
All Executive Directors are responsible for implementing records management arrangements at Directorate level through the relevant committees and meeting forums and overseeing a programme of record management activities, in accordance with this policy.

Digital Director
The Digital Director is responsible for ensuring that regulations are in place to maintain the security of all electronically stored information, outlining the security responsibilities of management and staff. The Director is also responsible for the management of electronic/digital systems.

Information Governance Sub Committee
The Information Governance Sub Committee is responsible for ensuring that the Health Records Management Policy is implemented through its endorsement and approval and will take a lead role in its obligation to ensure robust records management arrangements are implemented across the HDUHB.

Head of Information Governance
The Head of Information Governance is the designated management advisor for the HDUHB and has responsibility for ensuring that the HDUHB complies with the developments in national guidance relating to information governance. They will have a responsibility to provide any specialised advice or guidance to other service areas as required and maintain an Information Asset register, which can be utilised for records management arrangements.

Health Records Manager
The Health Records Manager has professional responsibility and accountability for the overall development and maintenance of health records management practices within the organisation and for ensuring that related policies and procedures conform to the latest legislation and standards on data protection, UK GDPR, confidentiality and health records practice. They will have a responsibility to

provide specialised leadership, guidance, advice and support in regards records management arrangements and processes within the HDUHB. They have responsibility for overseeing, directing and coordinating the day to day management of operational matters within the Health Records Service including the provision of patient records for inpatient, outpatient and day case attendances. They are responsible for ensuring that the release of all patient clinical information for data Subject Access Requests (SARs) and provision of records for medico-legal purposes is in accordance with the legislation.

Information Asset Owners & Information Asset Administrators
Information Asset Owners (IAO's) will delegate responsibility to Information Asset Administrators (IAA's), whose remit will also include responsibility for health record management arrangements within their service. The IAO's will ensure that the policy is implemented within their service areas and robust records management arrangements are in operation.

Professional Staff Groups
Professional staff groups must ensure that they maintain factual, clear, concise and unambiguous records to provide credible and authoritative evidence of services delivered. They must ensure that all contact with service users, carers or other relevant individuals is systematically recorded in keeping with agreed standards. Ensure that no action or omission on their part or within their sphere of responsibility is detrimental to the interests, condition or safety of service users, staff or the HDUHB and that records are always documented with a view that they can potentially be disclosed and read by the service user/patient**.**

Employees
All NHS employees and staff are responsible for any health records which they create or use. This responsibility is established and defined by the law and any records created by an employee are public records. All HDUHB staff, whether clinical or administrative, have an individual responsibility for records management and for the correct creation, use and retention of records in line with their job roles. Staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any supporting policies or guidance subsequently produced.

Everyone working for or within the NHS who records, handles, stores or otherwise comes across patient information has a personal common law duty of confidence to patients and to his or her employer. The duty of confidence continues even after the death of the patient of after the employee or contractor has left the NHS. All staff must ensure that all confidential, patient identifiable information is retained in the appropriate records management system. Staff have a duty to read and understand the content of this policy and a Breach of this policy will mean that the HDUHB is not safeguarding information entrusted to it, which could render the HDUHB liable to prosecution. It is therefore essential that staff within the organisation with responsibility for record management comply with the policy or they may be subject to disciplinary procedures.

Legal and Professional Obligations

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. All NHS Health Records are public records under the Public Records Act. The HDUHB will take actions as necessary to comply with legal and professional obligations such as:

- Public Records Act 1958 and Local Government Act 1972
- Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2022
- UK GDPR and Data Protection Act 2018
- Access to Health Records Act 1990
- The Common Law Duty of Confidentiality
- Health and Social Act 2008
- Limitation Act 1980 and Consumer Protection Act 1987
- Caldicott: Principles into Practice
- Any new legislation affecting health records management as it arises

Health and care professionals also have professional responsibilities for example complying with the **record keeping standards** as set out by registrant bodies.

Health Records Lifecycle

Health records are confidential documents and should be clearly identifiable, accessible and retrievable. They should be authentic, meaningful, authoritative and adequate for their purpose and correctly reflect what was communicated, decided or done. They should be unalterable and after an action has occurred nothing from the health record should be deleted or altered. Information added to an existing hard copy health record should be signed and dated. Health records systems should be secure and their creation, management, storage and disposal should comply with current legislation.

Creation

A comprehensive health record is created and maintained for every patient attending health services to provide an up to date and chronological account of the patient's care.

- Patient demographic data for each registration should be recorded on the master patient index of the patient administration or departmental system
- The minimum patient demographic data should include: surname, forename, sex, date of birth, home address, postcode, NHS and or PAS/departmental number
- The organisation should use the NHS number as the main patient identifier and a partial validation tool
- Where there is more than one local identifier or case record per patient, a system is in place to ensure that the existence of all other health records is known
- The paper health record has a standard case record folder constructed of robust material which can withstand handling and transport and has secure anchorage points to protect against loss or damage to documentation
- There is a designated area within the health record for health professionals to record actual or suspected clinical alerts or risk factors
- There is a locally agreed format for the filing of the information in the health record which facilitates ease of access to all clinical information. Clear instructions regarding the order of filing is contained within the folder
- Machine generated reports and recordings such as CTG, ECG and laboratory reports are stored securely within the case note folder
- All electronic systems are password protected and passwords are changed at regular intervals. An audit trail of access, amendments or updates is available and reports can be taken from the system

Storage
Health record storage areas should provide a safe working environment with secure storage that allows health records to be retrieved as and when required. These areas should only be accessible to authorised staff and should conform to agreed standards e.g. BS 5454 to protect records from damp, fire, flood and chemical contamination.

- Health records storage areas and office accommodation should conform to all current legislation and guidance regarding health and safety
- Risk assessments are undertaken in line with the risk management strategy
- Racking, where this is in use, is stable and of strong enough construction to support the weight of the health records and mostly complies with current health and safety regulations
- There are safety step ladders and stools appropriate to the number of staff employed and to the size of the different storage areas
- The staff are trained in the manual handling procedures associated with the library areas
- Equipment within the department conforms to the appropriate legislation and equipment checks are conducted when necessary
- Access to the libraries is restricted to authorised personnel. The keys/access codes/swipes to areas that are locked are made available to staff to facilitate the retrieval of health records during the out-of-hours service
- The health records areas should be capable of accommodating the current needs and annual growth of health records
- Health records must be stored securely when in clinical areas, offices and arrangements made within these areas to allow retrieval of records when required

Management of Records (onsite & offsite)
Maintaining the health record is vital to patient care. The health records service has well defined procedures and systems in operation for the ongoing management of the health record from initiation to final disposal in accordance with legislation.

- Whenever possible, separate areas are maintained for current and non-current health records in use within the organisation;
- There are documented procedures for the safe storage and retrieval of health records;
- There are documented procedures for the tracking of records within the organisation and audit is used to highlight any issues that arise as a result of non compliance
- There is a documented procedure for the splitting of fat folders and cross referencing of the volumes. Closed volumes are suitably labelled.
- There is a documented procedure relating to the return of the patient held record when an episode of care is complete.
- The responsibility for the filing of loose documentation rests with the staff who generate the information.
- There are agreed processes and identified staff responsible for the filing of loose documentation.
- Each person who uses and adds to the record has the responsibility to maintain the record and file any information into the appropriate section and format. This is part of the overall record keeping standards of the organisation.
- Health records staff will routinely split large folders or provide a new folder if the outer cover is not of a good standard.
- There are documented procedures for the transportation of health records both within and outside of the HDUHB.

- There are documented procedures for the handling of subject access and Access to Health Records requests with clear responsibility for responding by fully trained, dedicated staff who process requests in accordance with the law;
- There are documented procedures for the retention, archiving and destruction of health records in accordance with national guidelines. The method of destruction ensures that confidentiality is maintained at all times.
- There is a set of performance indicators which demonstrate the efficiency of the health records service which include health record availability, incorrectly tracked records, SAR's compliance etc
- Offsite records requires that there is a full inventory of the records that are held offsite
- Retention periods require to be assigned to each record held offsite
- Evidence is obtained of secure disposal of records and information
- A Data Protection Impact Assessment (DPIA) must be conducted if moving records to an offsite storage contractor and the Health Records service contacted for advice and guidance on the factors to be taken into consideration prior to removal of records to an offsite store.

Creation and Maintenance of Patient Healthcare Records

The HDUHB uses the Welsh Patient Administration system (WPAS) to create a patient record. HDUHB policies and procedures specify clear standards that should used by all staff involved in maintaining the patient record.

Wherever possible all patient information should be centrally held as part of the main patient record. However the HDUHB acknowledges that in some circumstances it may be practical to generate or hold local patient records, for example emergency attendances. Where there are locally held patient records, all staff involved in the creation, use and/or management of these records should also ensure they meet the required standards and ensure that the record types are recorded on the Information Asset Register.

The Health Records Department are responsible for identifying main clinical records for retention or destruction and will apply the retention schedules as stipulated in the HDUHB 193 - Retention and Destruction Policy – opens in a new tab - and supported by the Record Management Code of Practice.

Tracking and Retrieval of Records

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with and that there is an auditable trail of record transactions.

The HDUHB utilises the Welsh Patient Admin System **Intelligent Tracking** facility to monitor and records the movement of the main patient healthcare record within the organisation (paper). The objectives of this policy are to:

- Ensure all health records are tracked on WPAS
- Ensure the location of all health records are known at all times
- Establish and maintain standards for the use of health records
- Reduce the risk of health records not being available for patient consultations, subject access requests and legal requirements

Archiving and Disposal of Health Records

There is a detailed and agreed policy on the retention, destruction and/or archiving of health records, which operates in accordance with the Welsh Records Management Code of Practice. It is particularly important that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies.

It is a fundamental requirement that all the HDUHB records are retained for a minimum period for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the HDUHB business and clinical functions. The HDUHB has a retention schedule which is set out in the HDUHB 193 - Retention and Destruction Policy – opens in a new tab. Records destroyed shall be recorded on WPAS. Destruction of eligible records shall be completed annually with archived records indicating the year for destruction, which will enable those pending destruction to be identified. Any decision to retain/destroy records outside of the periods specified will be approved and fully documented.

The Health Records Manager and Health Records Management team can offer advice on the requirements and procedure for dealing with the disposal of all records at this stage in the lifecycle.

Training

While some aspects of Information Governance is covered in the HDUHB Corporate Induction for all staff, it is expected that local induction arrangements will cover the specific roles and responsibilities of staff in relation to the lifecycle of records. All staff employed by the NHS in Wales will receive information on their personal responsibilities for record keeping in contracts of employment. This includes the creation, use, storage, security and confidentiality of health records. The mandatory training on Information Governance also includes elements of records management standards.

Appropriate training will be given to all health records staff on the systems used to maintain records and these will meet local and national standards. The Health Records service is able to support awareness sessions or bespoke sessions as and when required to increase the awareness of individual staff responsibilities in regards records management. Self-learning modules are available to all staff through the HDUHB's intranet and ESR application.

GIG CYMRU NHS WALES | Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

Information Rights Procedure

Procedure information

Procedure number: 1088

Classification: Corporate

Supersedes: N/A

Version number:
1

Date of Equality Impact Assessment:
12/07/2022

Approval information

Approved by:
Sustainable Resources Committee

Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
The aim of this document is to give clear guidance to patients, staff and the Information Governance Team about the process for managing an individual's information rights under the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

Scope:
This procedure applies to and must be followed by all staff across the Hywel Dda Health Board. It applies to information requests made for any personal information processed by the Health Board.
Requests could be made by staff members, patients, relatives of patients regarding personal information processed about them.
It applies to both electronic and hard copy (paper) information.

To be read in conjunction with:
172 – Confidentiality Policy Opens in a new tab
836 – All Wales Information Governance Policy Opens in a new tab

224 – Access to health Records Policy Opens in a new tab

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub Committee
24/10/2022 / 08/04/2023

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1.0 New Procedure

Keywords
Information Governance, Data Protection, Right of Access, Subject Access Request, How to access my personal information, Information Rights

Glossary of terms

Term	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
Data Protection Legislation DPA 18	Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.
Data Protection Officer	Is the Health Board's lead and main contact for all data protection issues.
Information Asset Owner	Are senior individuals within the Health Board who have been identified to take responsibility for ensuring that Information Assets are handled and managed appropriately within their respective departments or service areas.
Information Commissioner's Office (ICO)	The UK independent regulator set up to uphold information rights.
Information sent securely	Electronically – information will be sent via Secure File Share Portal Hard copy/paper – information will be posted and tracked via Royal Mail Recorded or Special Delivery
Personal Data / Personal Information	Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as patients or service users.
Senior Information Risk Owner (SIRO)	An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board.

UK GDPR	UK General Data Protection Regulation
Unauthorised Access	Access to information that is not part of your work duties. Access to a patients record where the patient is not under your care.
Unauthorised individual	Individual who does not have a valid or legitimate reason for having access to information either a staff member or member of the public.

Table of Contents

Scope

This procedure applies to and must be followed by all staff across the Hywel Dda Health Board. It applies to information requests made for any personal information processed by the Health Board.

Requests could be made by staff members, patients, relatives of patients regarding personal information processed about them.

Aim

The aim of this document is to:

- ensure that the Health Board manages the Individual's Information Rights in line with the UK General Data Protection Regulation (GDPR) and the Data Protection Act.
- ensure that all staff understand their responsibilities when provide guidance they receive Information Rights requests.

Objectives

The aim of this document will be achieved by the following objectives:

- Ensuring that all staff recognise and understand the Individual's Information Rights.
- Ensuring that all staff understand their responsibilities and the process that must be followed should they receive a request under Information Rights.
- Ensuring that all members of the Information Governance Team understand the process to be followed when managing an Information Rights request.
- Ensuring that the Information Governance Team continually reviews the process for managing an individual's Information Rights and implements appropriate improvements, where necessary.
- Ensuring the Health Board is meeting its legal requirements in relation to the Data Protection Legislation.

What are the Individual's Information Rights?

The UK General Data Protection Regulations (GDPR) together with the Data Protection Act 2018, update and strengthen an individual's information rights.

Under Chapter 3, Articles 13 to 22 of the UK GDPR, an individual has certain rights that they can exercise in relation to the personal information an organisation processes about them. All requests to exercise an information right must be dealt without undue delay.

The below rights are available to be exercised by the individual, however, they could also be applied by a third party acting on behalf of the individual. For example, a parent on behalf of a child or a solicitor on behalf of their client. If this is the case, contact the IG team for advice on how to validate and proceed with this request.

The Right to be Informed

Articles 12-14 of the UK GDPR provide the individual's right to be informed. Under this right, the Health Board must inform data subjects if and how we are using their personal data, by providing the below detailed 'Privacy Information' at the time we start to use or collect it, we do this by issuing a Privacy Notice which covers the following points:

- Why we use their data.
- The lawful basis for the processing of their data.
- What type/types of data we use.
- Where the data is from.
- How long their data will be kept.
- Whether we will be sharing data to third parties, including their names and the reasons for the sharing.
- Whether we transfer the data overseas, including the country involved and what will be done with the data.
- Whether we use the data in profiling (a type of automated processing where personal data is used to analyse or predict things such as performance at work, economic situation, health, personal preferences and interests).
- Their information rights.
- How to contact us.
- Their right to complain to the ICO

What staff need to do: All service areas should consider whether they are complying with this right, and whether there is anything more they can do to ensure transparency with our staff and patients in regard to what we do with their information.

Examples of how we can comply with this right, include:

- Our Patient Privacy Notice - Opens in a new tab
- Our Employee Privacy Notice – Opens in a new tab -On main HDUHB Website the notice applies to current and former employees, workers and contractors.
- Your Information, Your Rights – Opens in a new tab - generic NHS Wales privacy poster/leaflet for use in public facing spaces throughout the Health Board.
- Children's Privacy Notice Video - Opens in a new tab -found under 'Your Information, Your Rights' on our external website or on our YouTube channel - Opens in a new tab.
- Departmental Privacy Posters – developed by each service area and displayed in public facing spaces throughout the Health Board.
- Bespoke Service Information – these are leaflets or information sheets that could be provided to patients as they get involved in your service area, informing them of what you do with their personal data. IG can help you develop these.
- Face-to-Face Discussion – informing patients of what is happening to them is a key area of providing clinical care. Part of this discussion should include what we do with their personal information.

Bilingual copies of the above templates, along with support and advice on developing bespoke service level privacy information, is available on request from the IG Team.

The Right of Access

Article 15 of the UK GDPR provides the individual's right to access. Individuals have the right to find out if we are using or storing their personal data. They can exercise this right by asking for a copy of the information, which is commonly known as making a 'Subject Access Request'. Under ICO guidance, an individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. It's also worth noting that individuals aren't required to use the technical term for a request ('SAR' or 'subject access request').

If a member of staff receives a request that they believe is for personal information or an individual exercising any of the above information rights, they should direct to the teams below to manage.

Request for Medical Information / Health Records:

- Via email to access.healthrecords.hdd@wales.nhs.uk
- Via post to Access to Health Records, Hywel Dda University Health Board, Amman Valley Hospital, Folland Road, Glanamman, Ammanford, Carmarthenshire, SA18 2BQ

Please see the 249 - Access to Health Records Policy for more information - Opens in a new tab.

Request for other Personal Information (Corporate / non-Medical Records / staff records):

- Via email to information.governance.hdd@wales.nhs.uk
- Via phone to 01437 773969/70/17
- Via post to Information Governance, IT Building, Withybush General Hospital, Haverfordwest, Pembrokeshire, SA61 2PZ

If staff are not sure whether the request is for personal information held within a health record or corporately, they should contact the Information Governance Team for advice

The Information Governance Team will follow the flow chart in Appendix A to manage Subject Access Requests for corporate / non-medical personal information requests. In summary, the IG team will:

- Use all reasonable measures to be sure that the person making the request is entitled to the information and specify the information to which the request relates.
- Acknowledge request and log on the IG SAR tracker at all relevant activity points
- Liaise with relevant department to collate information
- Process the request, consider any relevant exemptions and redact (remove) any information, as necessary.
- Ensure request is authorised for release before sending the information to the data subject.
- If the data subject requests an Internal Review, the IG team will manage this process with oversight of the Data Protection Officer.

The internal process for managing a Subject Access Request is detailed in Appendix B.

Exemptions to the Release of Information

The Health Board is committed to complying with SARs. There are, however, occasions when an SAR may be refused, or timelines to respond to a SAR extended. The UK GDPR and DPA ICO guidance should be followed in such cases, in consultation with the Health Board's Data Protection Officer (DPO).

There are several exemptions that are set out under the Data Protection Act 2018 which allow information to be withheld from the individual that has made the request. Some of the current exemptions include the following:

- you believe that disclosure of the information is likely to cause serious physical or mental harm to the individual or another person
- confidential references provided by an employer in support of a person's application for employment are exempt from SARs
- employers do not have to disclose information which relates to legal advice or legal proceedings as this is covered by legal professional privilege
- personal data which relates to management information such as management forecasting.

In addition, you do not have to provide a person with a copy of their health and care records if you believe their subject access request is "manifestly unfounded or excessive". Or should you choose to respond you may charge a reasonable fee for doing so. Subject access requests that fall into this category are likely to be repetitive (for example, regular requests for copies of records especially where there has been little or no change to the record since the previous request), aimed at disrupting your organisation or targeted against an individual. Decisions about whether an SAR falls into this category must be taken on a case-by-case basis and we must be able to justify our decision with evidence.

Third party Subject Access Requests

Individuals can authorise third parties (for example, solicitors) to make a SAR on their behalf. Health and care providers releasing information to solicitors acting for their patients and service users should ensure they have the individual's written consent.

The Right of Rectification

Article 16 of the UK GDPR provides the individual's right to rectification. Individuals have the right to challenge the accuracy of the personal data we hold about them and ask for incorrect information to be amended, or incomplete information completed.

If a request for rectification is received reasonable steps should be taken to be satisfied that the data is accurate and to rectify the data if necessary. Evidence and arguments provided by the individual should be taken into consideration. What steps are reasonable will depend, in particular, on the nature of the personal information and what it will be used for. The more important it is that the personal data is accurate, the greater the effort necessary to check its accuracy and, if required, the steps taken to rectify it. For example, more effort should be made to rectify inaccurate personal information if it is used to make significant decisions that will affect an individual or others, rather than trivial ones. Steps already taken to verify the accuracy of the information prior to the challenge by the individual should also be taken into account.

If the information is recorded as part of the individual's health record, this often cannot be amended as it stands as a matter of record. It can also be complex where the information in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. Where rectification is refused on these grounds, we can still comply with this right by adding a supplementary or correction note to the record, highlighting the individual's view of what information they dispute as incorrect.

If the personal information in question has been disclosed to third parties, they must be informed of the rectification where possible. For example, where an amendment has been made to a referral to another Health Board or GP.

What staff need to do: Follow flow chart in in Appendices C to manage the request within your service area. If you are unable to process informally or for more complex requests, forward to the Information Governance Team.

The Right to Erasure

Article 17 of the UK GDPR provides the individual's 'Right to erasure' or known as the 'right to be forgotten'. Under this right individuals can ask us to delete personal data that we hold about them.

The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

Examples of when we can comply, include:

- If we no longer need the data, in line with our retention guidelines;
- If the individual consented for us to use their data and have now withdrawn their consent;
- If they have objected to the use of their data, and their interests outweigh ours for using it; or
- We have collected or used the data unlawfully.
- If we have to do it to comply with a legal obligation

What staff need to do: Always seek advice from the Information Governance Team in relation to all erasure or restriction requests before deleting any data.

Right to Restrict Processing

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

Examples of when we can comply, include:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;

- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

As a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

Right to Data Portability

Article 20 of the UK GDPR provides the individual's right to data portability. This is similar to the right of access, but information is provided in an accessible and machine-readable format, like a csv file. Individuals can also ask for this to be transferred to another organisation, if the transfer is 'technically feasible'.

This is not an absolute right and only applies to information that is held electronically, and has been provided to the Health Board by the individual or gathered from monitoring activities using a device or service, like a health/fitness app. It also only applies when we process data under a specific legal basis.

What staff need to do: Follow flow chart in in Appendices C.

Right to Object and Rights related to automated decision-making including profiling

Article 21 of the UK GDPR provides the individual's right to object to how we use their data. Individuals can also ask for human involvement in decisions made about them when their data is wholly processed by automated means (Article 22).

These rights are not absolute and there are only certain circumstances in which we can comply.

Examples of when the individual can object, include if we process their data:

- For a task carried out in the public interest;
- In our legitimate interests;
- For scientific or historical research, or statistical purposes; or
- For direct marketing.

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

What staff need to do: Follow flow chart in Appendices C. If you carry out any automated individual decision-making processes within your service area, ensure it is included on your Information Asset Register and notify the Information Governance Team for information. In addition, If you intend to use the children's personal data for the purposes of profiling children or making automated decisions about them then you must do a DPIA to establish whether your processing will result in a high risk to their rights and freedoms, please contact Information Governance team for advice.

The Right to Raise a Concern

Hywel Dda University Health Board takes the management of personal data seriously. We want all staff and patients to be confident that we have handled their information responsibly and in line with good practice.

An individual may have concerns with the way we are handling their personal data, like:

- Not keeping personal data secure;
- Holding inaccurate data;
- Disclosing information in error;
- Keeping information longer than necessary; or
- Collected for one purpose and using it for something else.

The Health Board has a responsibility to take these concerns seriously and should work with the individual to resolve their concern. All concerns raised about our personal data processing should be forwarded directly to the Information Governance Team to deal with. Where appropriate, more serious concerns will be managed by the Data Protection Officer.

If it is found that we have mishandled an individual's personal data, there are other rights that the individual can exercise, including:

- Article 77 – **the Right to lodge a complaint with the ICO**. If the data subject considers that the processing of personal data relating to them infringes legislation, they can lodge a complaint directly with the ICO.
- Article 78/79 – **the Right to an effective judicial remedy**. The data subject can challenge a legally binding decision made by the ICO concerning them or if they consider that their rights have been infringed as a result of the processing by a Controller or Processor in non-compliance with legislation, they can apply via the Courts.
- Article 82 – **the Right to compensation and liability**. A person who has suffered material or non-material damage as a result of an infringement of the legislation has the right to apply via the Courts to receive compensation from the Controller or Processor for the damage suffered.

What staff need to do: If you receive a compliant or concern from an individual about how the Health Board has processed their personal information, please forward directly to the Information Governance Team to manage.

Internal Processing of Information Rights by the IG Team

The Information Governance Team will follow the flow chart in Appendix C to manage requests to exercise the individual's information rights. In summary, the IG team will:

- Use all reasonable measures to verify the individual's identify and specify the information to which the request relates.
- Acknowledge request and log on the IG tracker at all relevant activity points.
- Liaise with and provide advice to the service area lead, where necessary.
- Process the request, consider the lawful processing of the personal data and any relevant exemptions and apply, as necessary.
- Ensure each request is authorised before completion.
- If the data subject raises a concern about how their personal data has been processed or requests an Internal Review, the IG team will manage this process with oversight of the Data Protection Officer.

Responsibilities

All Staff

- Be able to recognise a request where an individual is exercising their information rights.
- Follow this Standard Operating Procedure when complying with information rights.
- Seek advice from the Information Governance team, where necessary.

Information Asset Owners

- Ensure that all staff within their service area understand their responsibilities in relation to this Standard Operating Procedure.
- Promote a culture of good information governance and encourage all staff within their service areas to make sure information is recorded accurately and kept up to date.
- Ensure a relevant manager has oversight of all requests for personal information they hold within their service.

Access to Health Records (A2HR)

- Forward any requests received for Third Party access to personal information contained in or as part of Health Records request to the A2HR Team.
- Forward any requests received for personal information not contained in Health Records only to the IG Team.
- If a request includes both health and corporate personal information, the receiving team will take the lead and link in with the other team to coordinate the other element, as appropriate.
- A2HR Team will follow the 249 - Access to Health Records Policy for the internal processing of SARs for health information.
- Support and advise staff in their compliance with information rights.

Information Governance (IG) Teams

- Support and advise all staff in their compliance with information rights.
- Validate requests received for Third Party access to personal information contained in or as part of Health Records request for the A2HR Team to process.
- IG Team will follow this procedure for the internal processing of SARs for corporate information.
- Forward any requests received for personal information contained in Health Records only to the A2HR team.

Data Protection Officer

- Receive requests for an Internal Review where an individual has raised a concern regarding the processing of their personal data.
- Oversee all Internal Reviews and provide advice, where necessary.
- Respond to the data subject in regard to the Internal Review outcome.

Reporting Structures

The Information Governance Sub-Committee will function as the primary reporting and decision-making group in relation to all Individual Information Right requests. Statistics on the number received, any Internal Reviews and appeals to the ICO will be reported to the IGSC quarterly.

Requirements of Data Processors

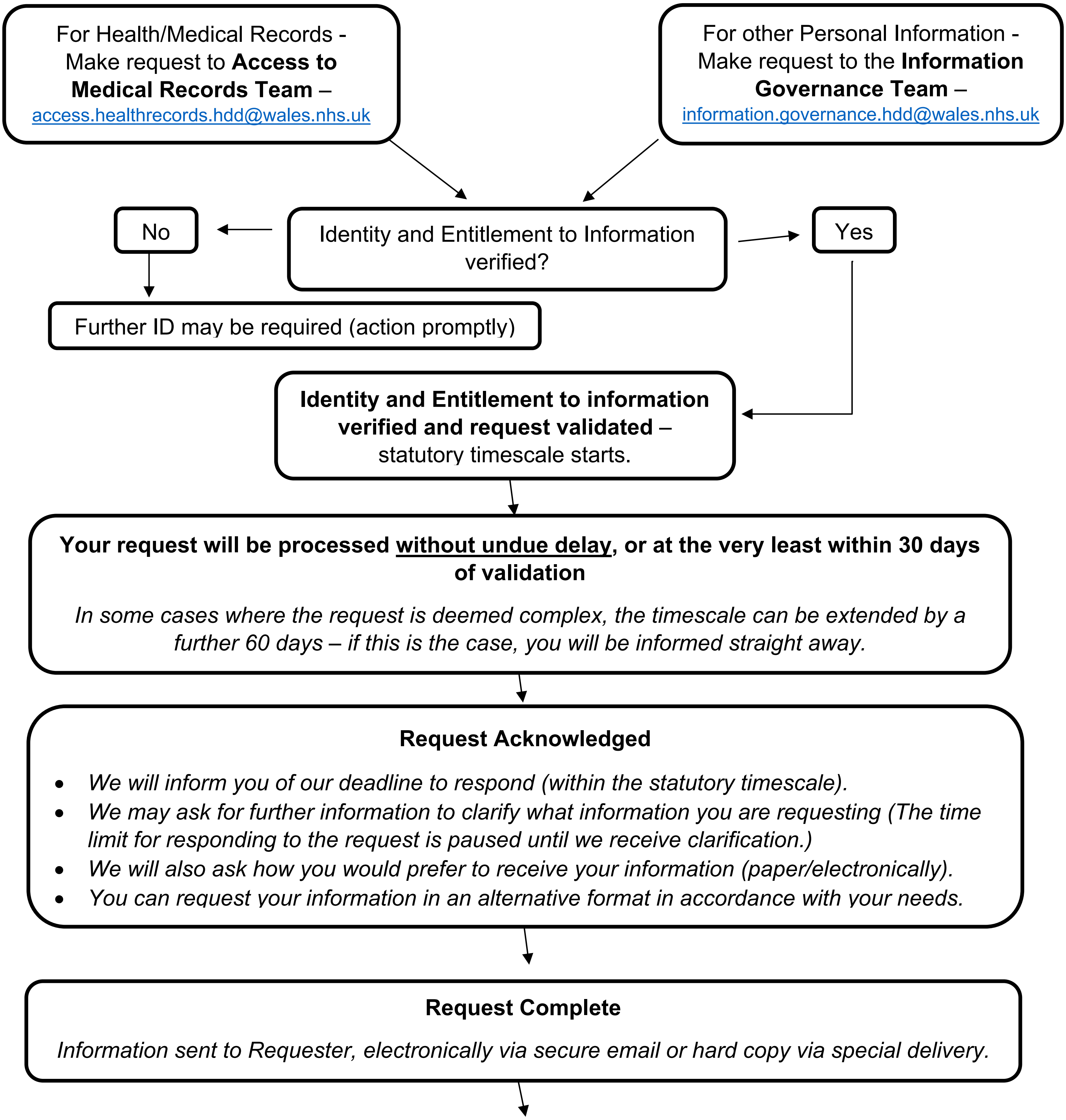
Where the Health Board are entering into any contract or agreement with a Data Processor to provide a service on its behalf and the processor are holding personal identifiable information, they will be required to manage any requests from a data subject to exercise any of their individual information rights without undue delay and within statutory timescales and report to the Health Board, where necessary.

References

Information Commissioner Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ Opens in a new tab

Appendix A

How to Make a Request for Personal Information to the Health Board



For Health/Medical Records - Make request to **Access to Medical Records Team** – access.healthrecords.hdd@wales.nhs.uk

For other Personal Information - Make request to the **Information Governance Team** – information.governance.hdd@wales.nhs.uk

Identity and Entitlement to Information verified?

No

Further ID may be required (action promptly)

Yes

Identity and Entitlement to information verified and request validated – statutory timescale starts.

Your request will be processed <u>without undue delay</u>, or at the very least within 30 days of validation

In some cases where the request is deemed complex, the timescale can be extended by a further 60 days – if this is the case, you will be informed straight away.

Request Acknowledged

- *We will inform you of our deadline to respond (within the statutory timescale).*
- *We may ask for further information to clarify what information you are requesting (The time limit for responding to the request is paused until we receive clarification.)*
- *We will also ask how you would prefer to receive your information (paper/electronically).*
- *You can request your information in an alternative format in accordance with your needs.*

Request Complete

Information sent to Requester, electronically via secure email or hard copy via special delivery.

If you are dissatisfied with how your request has been handled or have any queries about the information you have received, you can ask for an internal review.

- *To request an internal review you need to contact the Data Protection Officer, who is the Health Board lead on Data Protection.*

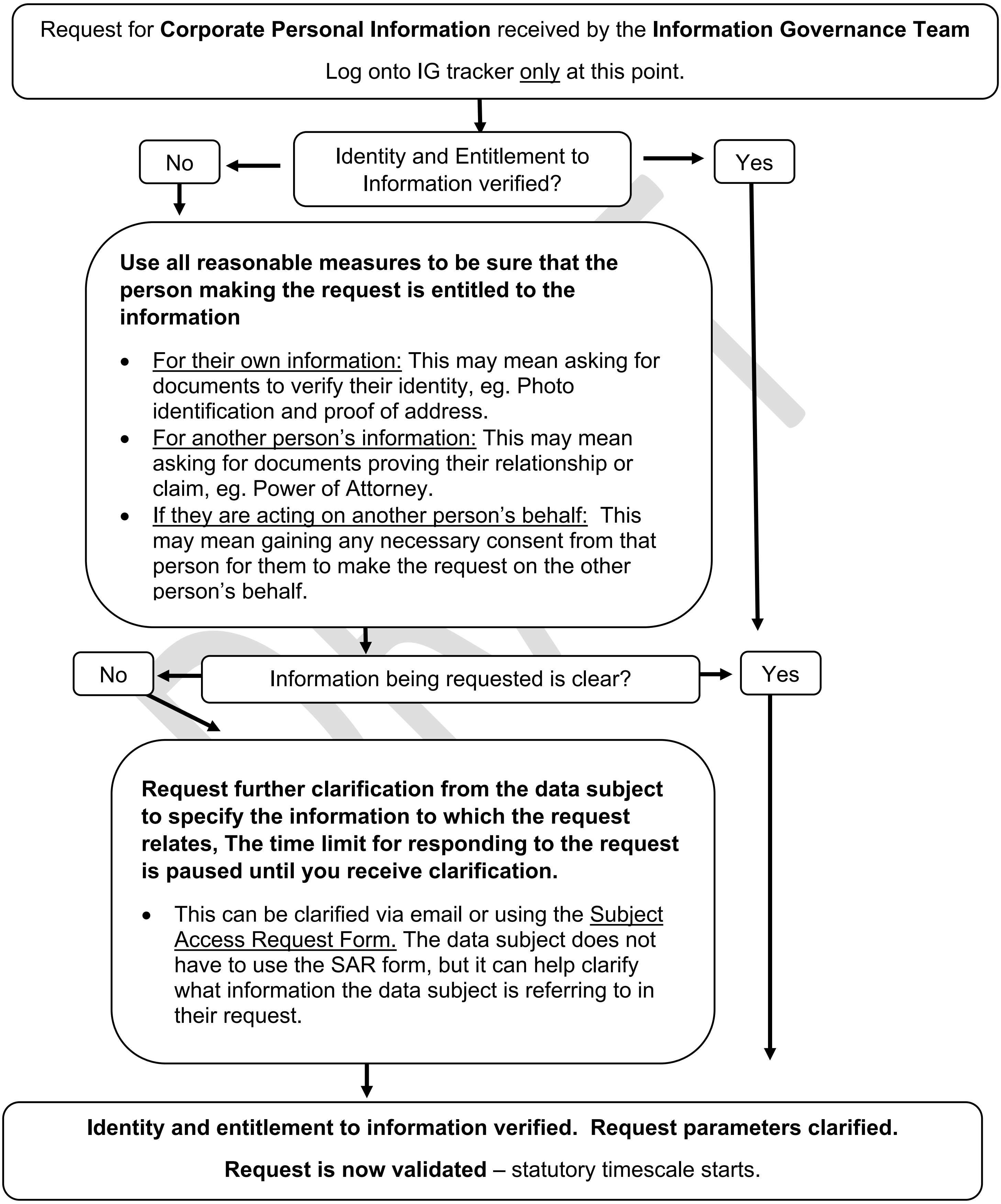
If you are not satisfied following the outcome, you have the right to complain to the ICO.

- *To make a complaint you need to contact the Information Commissioner, who is the statutory regulator.*
- *You do not have to request an internal review before appealing to the Information Commissioner, you have the right to make an appeal at any stage.*

APPENDIX B

Internal Process for Managing Corporate SARs

Process Step 1: Receipt and Validation of new Request



Request for **Corporate Personal Information** received by the **Information Governance Team**

Log onto IG tracker only at this point.

Identity and Entitlement to Information verified?

No

Yes

Use all reasonable measures to be sure that the person making the request is entitled to the information

- For their own information: This may mean asking for documents to verify their identity, eg. Photo identification and proof of address.
- For another person's information: This may mean asking for documents proving their relationship or claim, eg. Power of Attorney.
- If they are acting on another person's behalf: This may mean gaining any necessary consent from that person for them to make the request on the other person's behalf.

Information being requested is clear?

No

Yes

Request further clarification from the data subject to specify the information to which the request relates, The time limit for responding to the request is paused until you receive clarification.

- This can be clarified via email or using the Subject Access Request Form. The data subject does not have to use the SAR form, but it can help clarify what information the data subject is referring to in their request.

Identity and entitlement to information verified. Request parameters clarified.

Request is now validated – statutory timescale starts.

Process Step 2: Acknowledgement of Request

Request Logged

- Log request on the IG SAR tracker and allocate reference number.
- Save correspondence and request in a new SAR folder for the request.

Work Out Statutory Timescale

- Requests should be processed without undue delay.
- Record deadline – 30 days from date that the request was validated – on SAR tracker.
- In some cases where the request is deemed complex, the timescale can be extended by a further 60 days – if this is the case, justification should be recorded and the data subject informed within 30 days.

Request Acknowledged

- Send acknowledgement (in writing) to the data subject in the manner they made the request (via email/letter).
- Inform them of the deadline within which we have to respond (the statutory timescale).
- Confirm how they would like to receive their information (paper/electronically).
- Record on SAR tracker and save copy of correspondence in relevant folder.

Process Steps 3: Collate Information from relevant department

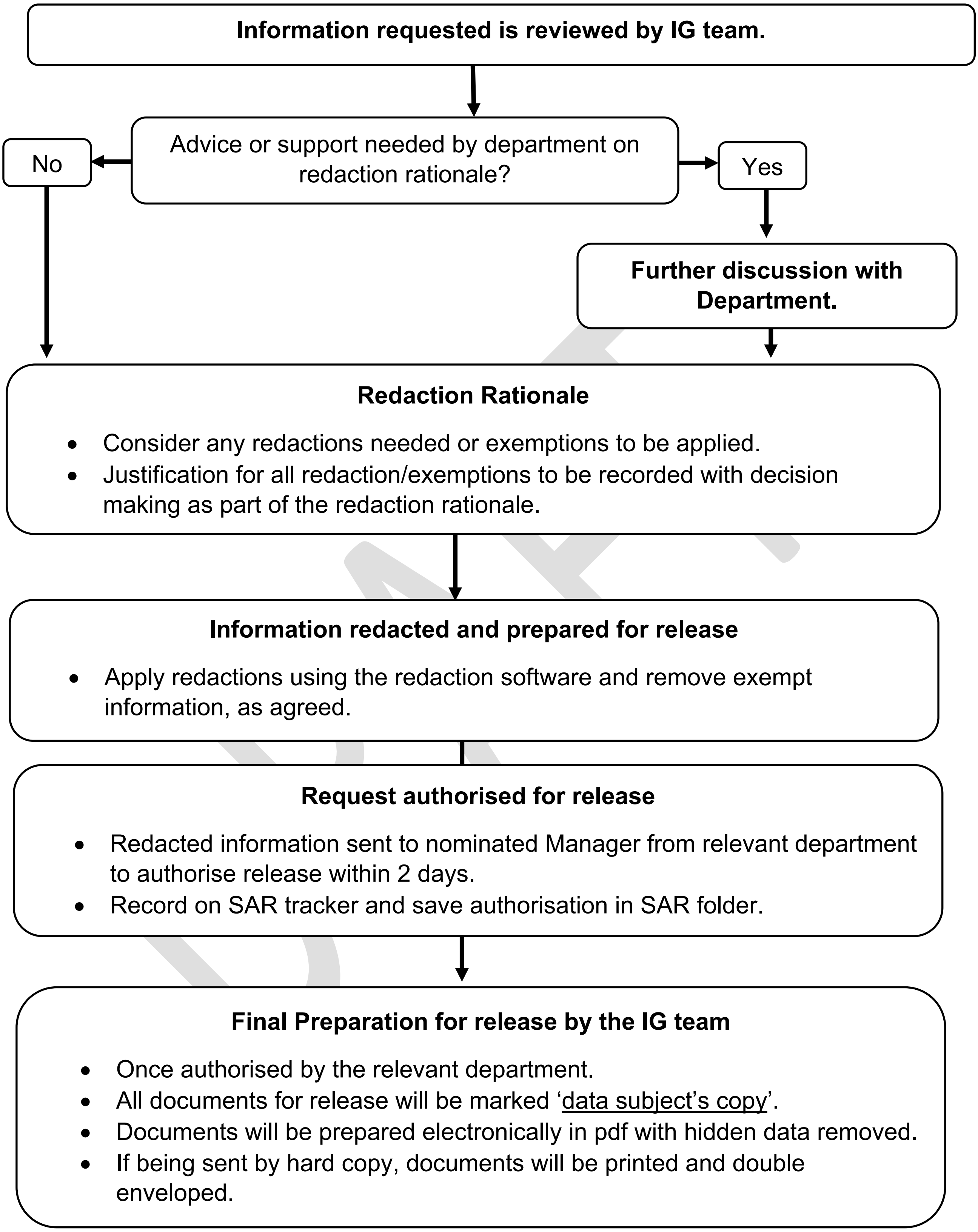
Request sent to relevant department

- Send ‘request for information’ document to the relevant department.
- Timescale set for response will be one week before deadline for release to give time to process/prepare for release.
- Record on SAR tracker and save correspondence in SAR folder.

Information requested is collated by department.

Information requested sent to IG team for review.

Process Steps 4: Process Request



Information requested is reviewed by IG team.

Advice or support needed by department on redaction rationale?

No

Yes

Further discussion with Department.

Redaction Rationale

- Consider any redactions needed or exemptions to be applied.
- Justification for all redaction/exemptions to be recorded with decision making as part of the redaction rationale.

Information redacted and prepared for release

- Apply redactions using the redaction software and remove exempt information, as agreed.

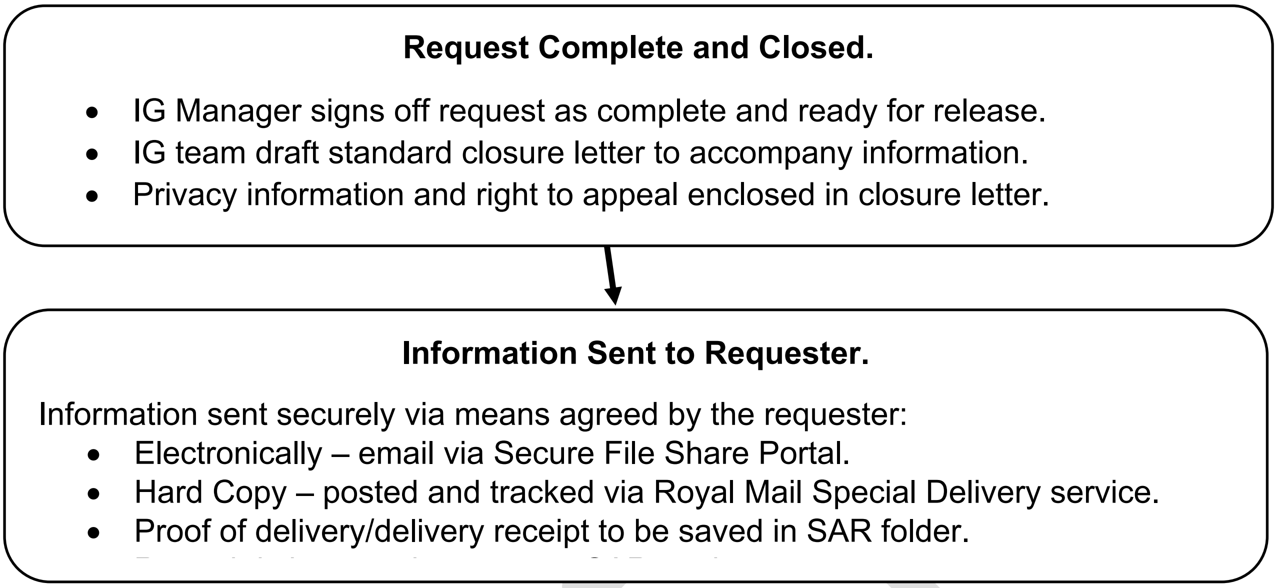
Request authorised for release

- Redacted information sent to nominated Manager from relevant department to authorise release within 2 days.
- Record on SAR tracker and save authorisation in SAR folder.

Final Preparation for release by the IG team

- Once authorised by the relevant department.
- All documents for release will be marked '<u>data subject's copy</u>'.
- Documents will be prepared electronically in pdf with hidden data removed.
- If being sent by hard copy, documents will be printed and double enveloped.

Process Step 5: Complete Request and Respond to Data Subject



Request Complete and Closed.

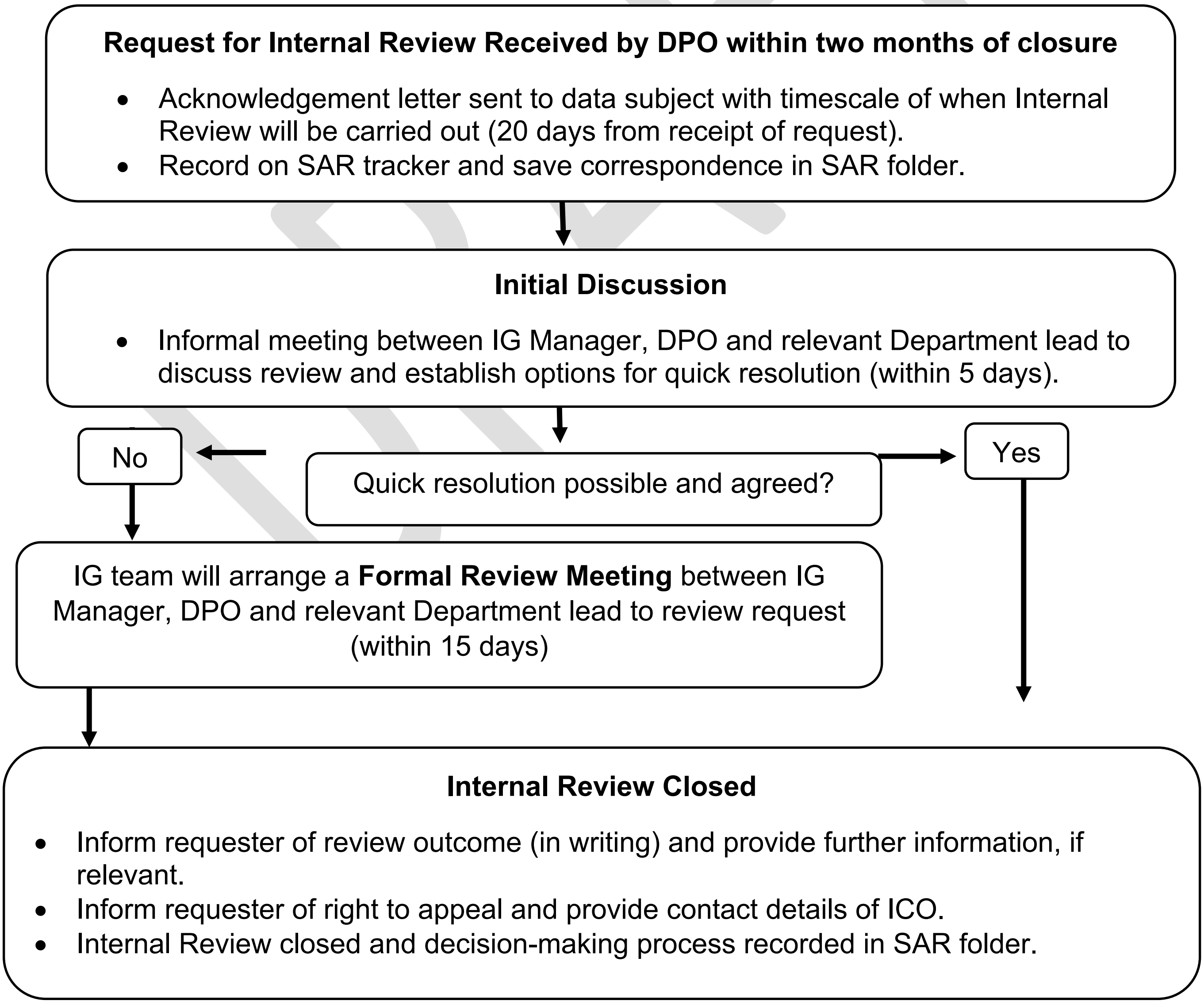
- IG Manager signs off request as complete and ready for release.
- IG team draft standard closure letter to accompany information.
- Privacy information and right to appeal enclosed in closure letter.

Information Sent to Requester.

Information sent securely via means agreed by the requester:

- Electronically – email via Secure File Share Portal.
- Hard Copy – posted and tracked via Royal Mail Special Delivery service.
- Proof of delivery/delivery receipt to be saved in SAR folder.

Process Step 6: Internal Review Process



Request for Internal Review Received by DPO within two months of closure

- Acknowledgement letter sent to data subject with timescale of when Internal Review will be carried out (20 days from receipt of request).
- Record on SAR tracker and save correspondence in SAR folder.

Initial Discussion

- Informal meeting between IG Manager, DPO and relevant Department lead to discuss review and establish options for quick resolution (within 5 days).

Quick resolution possible and agreed?

No

Yes

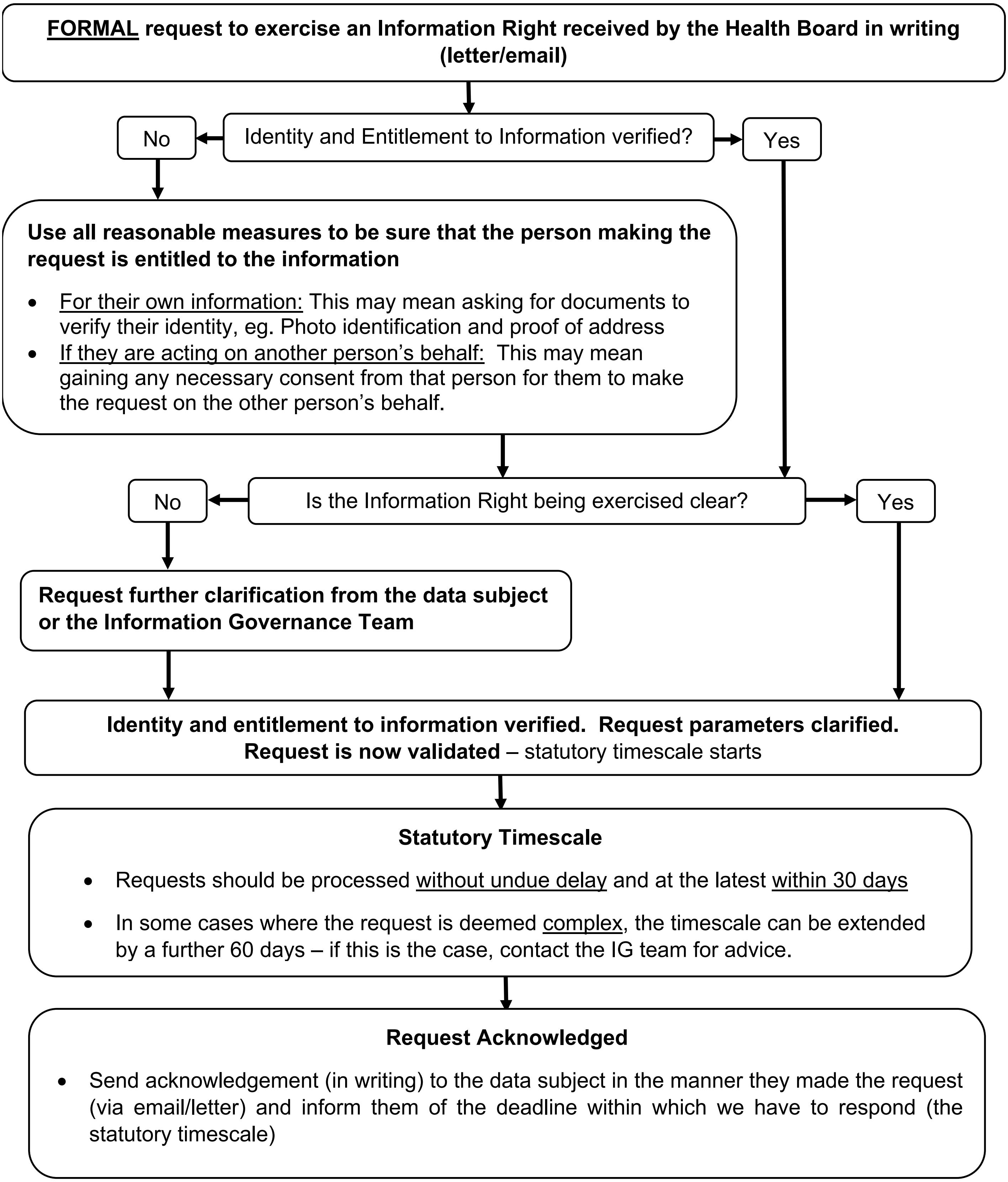
IG team will arrange a **Formal Review Meeting** between IG Manager, DPO and relevant Department lead to review request (within 15 days)

Internal Review Closed

- Inform requester of review outcome (in writing) and provide further information, if relevant.
- Inform requester of right to appeal and provide contact details of ICO.
- Internal Review closed and decision-making process recorded in SAR folder.

APPENDIX C

FORMAL Process for Managing Information Rights Requests



FORMAL request to exercise an Information Right received by the Health Board in writing (letter/email)

Identity and Entitlement to Information verified?

No

Yes

Use all reasonable measures to be sure that the person making the request is entitled to the information

- For their own information: This may mean asking for documents to verify their identity, eg. Photo identification and proof of address
- If they are acting on another person's behalf: This may mean gaining any necessary consent from that person for them to make the request on the other person's behalf.

Is the Information Right being exercised clear?

No

Yes

Request further clarification from the data subject or the Information Governance Team

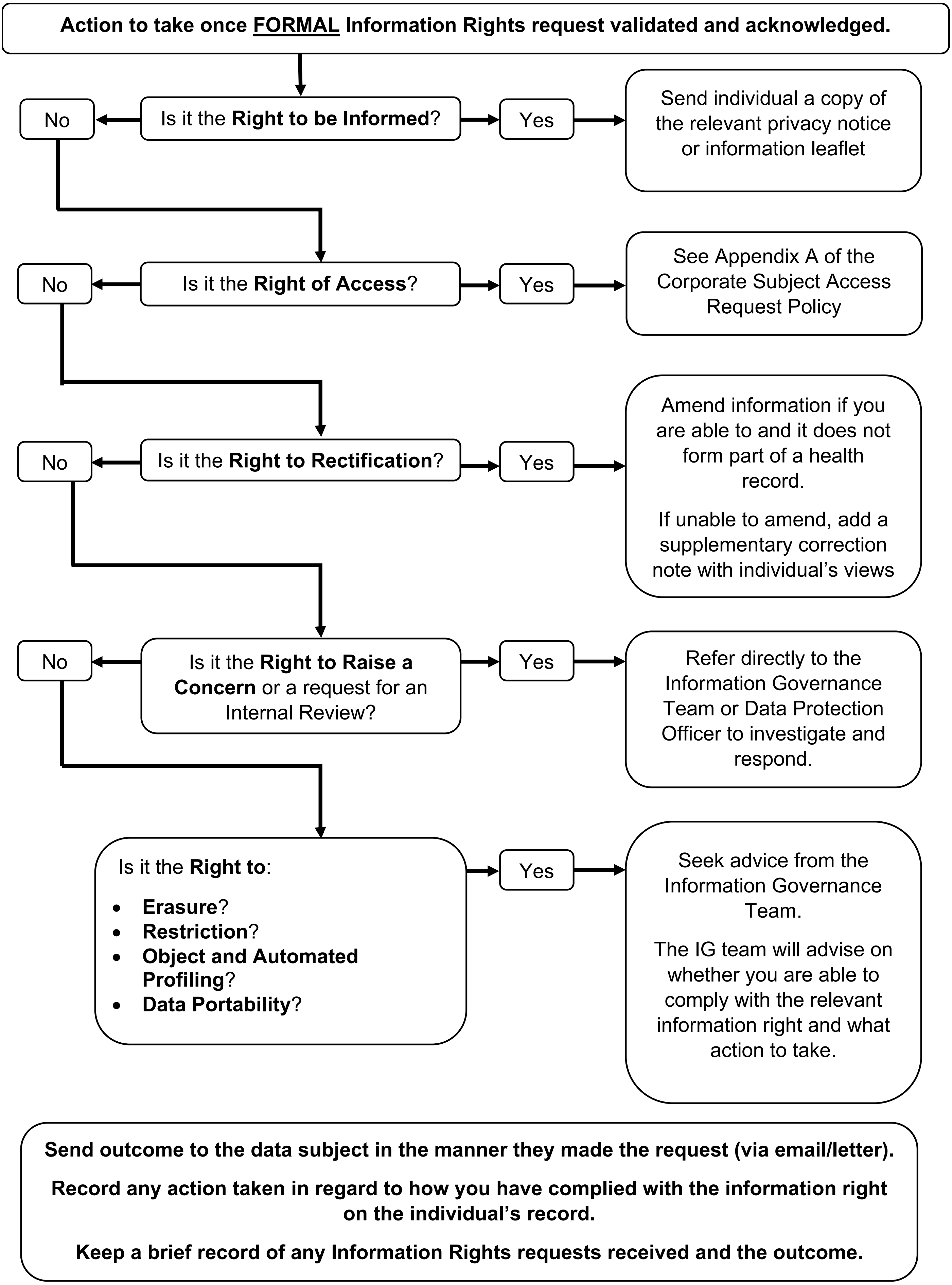
Identity and entitlement to information verified. Request parameters clarified.
Request is now validated – statutory timescale starts

Statutory Timescale

- Requests should be processed without undue delay and at the latest within 30 days
- In some cases where the request is deemed complex, the timescale can be extended by a further 60 days – if this is the case, contact the IG team for advice.

Request Acknowledged

- Send acknowledgement (in writing) to the data subject in the manner they made the request (via email/letter) and inform them of the deadline within which we have to respond (the statutory timescale)



Action to take once FORMAL Information Rights request validated and acknowledged.

Is it the **Right to be Informed**?

Yes → Send individual a copy of the relevant privacy notice or information leaflet

No

Is it the **Right of Access**?

Yes → See Appendix A of the Corporate Subject Access Request Policy

No

Is it the **Right to Rectification**?

Yes → Amend information if you are able to and it does not form part of a health record.

If unable to amend, add a supplementary correction note with individual's views

No

Is it the **Right to Raise a Concern** or a request for an Internal Review?

Yes → Refer directly to the Information Governance Team or Data Protection Officer to investigate and respond.

No

Is it the **Right to**:

- **Erasure**?
- **Restriction**?
- **Object and Automated Profiling**?
- **Data Portability**?

Yes → Seek advice from the Information Governance Team.

The IG team will advise on whether you are able to comply with the relevant information right and what action to take.

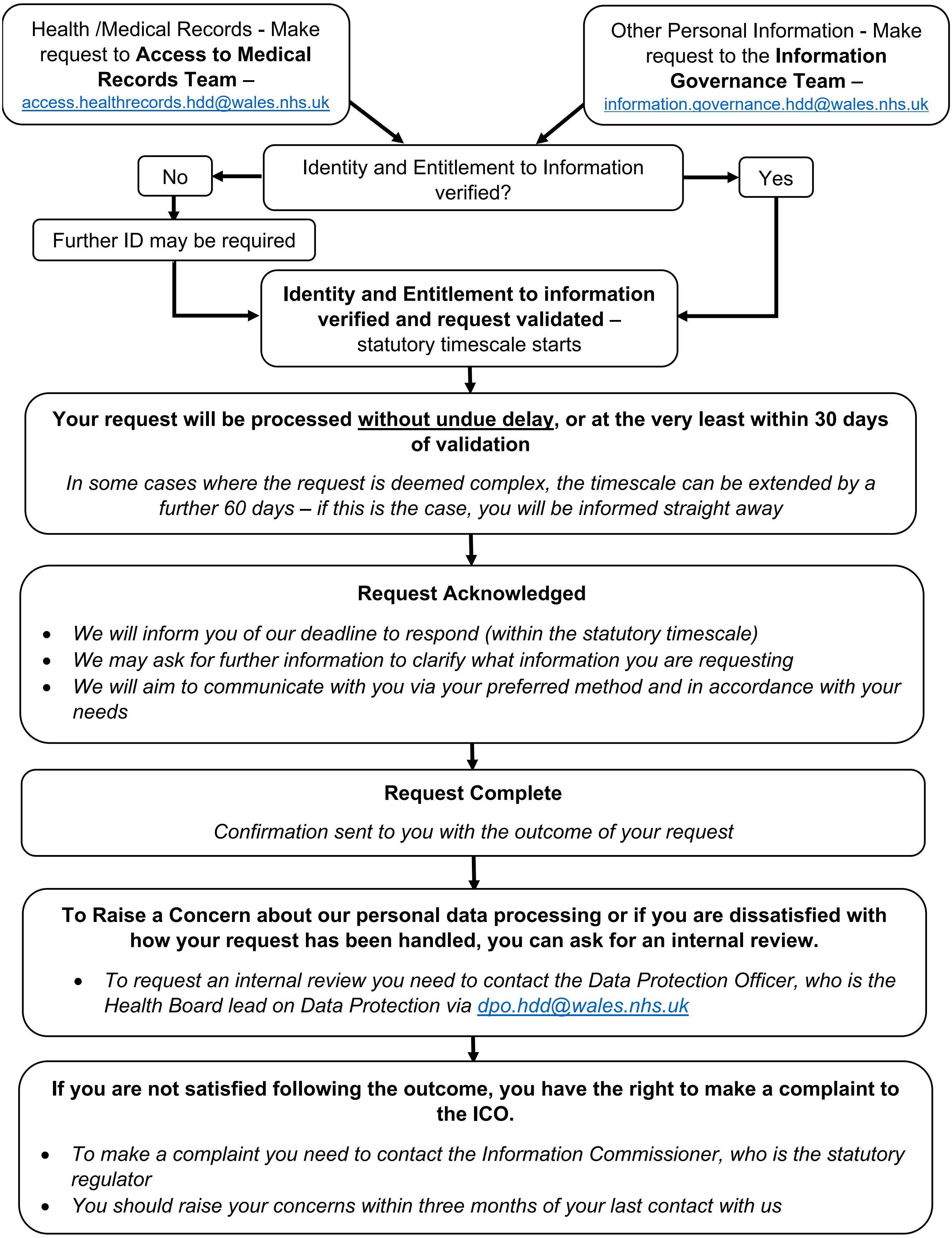
Send outcome to the data subject in the manner they made the request (via email/letter).

Record any action taken in regard to how you have complied with the information right on the individual's record.

Keep a brief record of any Information Rights requests received and the outcome.

APPENDIX D

How to exercise your Information Rights to the Health Board



Health /Medical Records - Make request to **Access to Medical Records Team –** access.healthrecords.hdd@wales.nhs.uk

Other Personal Information - Make request to the **Information Governance Team –** information.governance.hdd@wales.nhs.uk

Identity and Entitlement to Information verified?

No

Further ID may be required

Yes

Identity and Entitlement to information verified and request validated – statutory timescale starts

Your request will be processed <u>without undue delay</u>, or at the very least within 30 days of validation

In some cases where the request is deemed complex, the timescale can be extended by a further 60 days – if this is the case, you will be informed straight away

Request Acknowledged

- *We will inform you of our deadline to respond (within the statutory timescale)*
- *We may ask for further information to clarify what information you are requesting*
- *We will aim to communicate with you via your preferred method and in accordance with your needs*

Request Complete

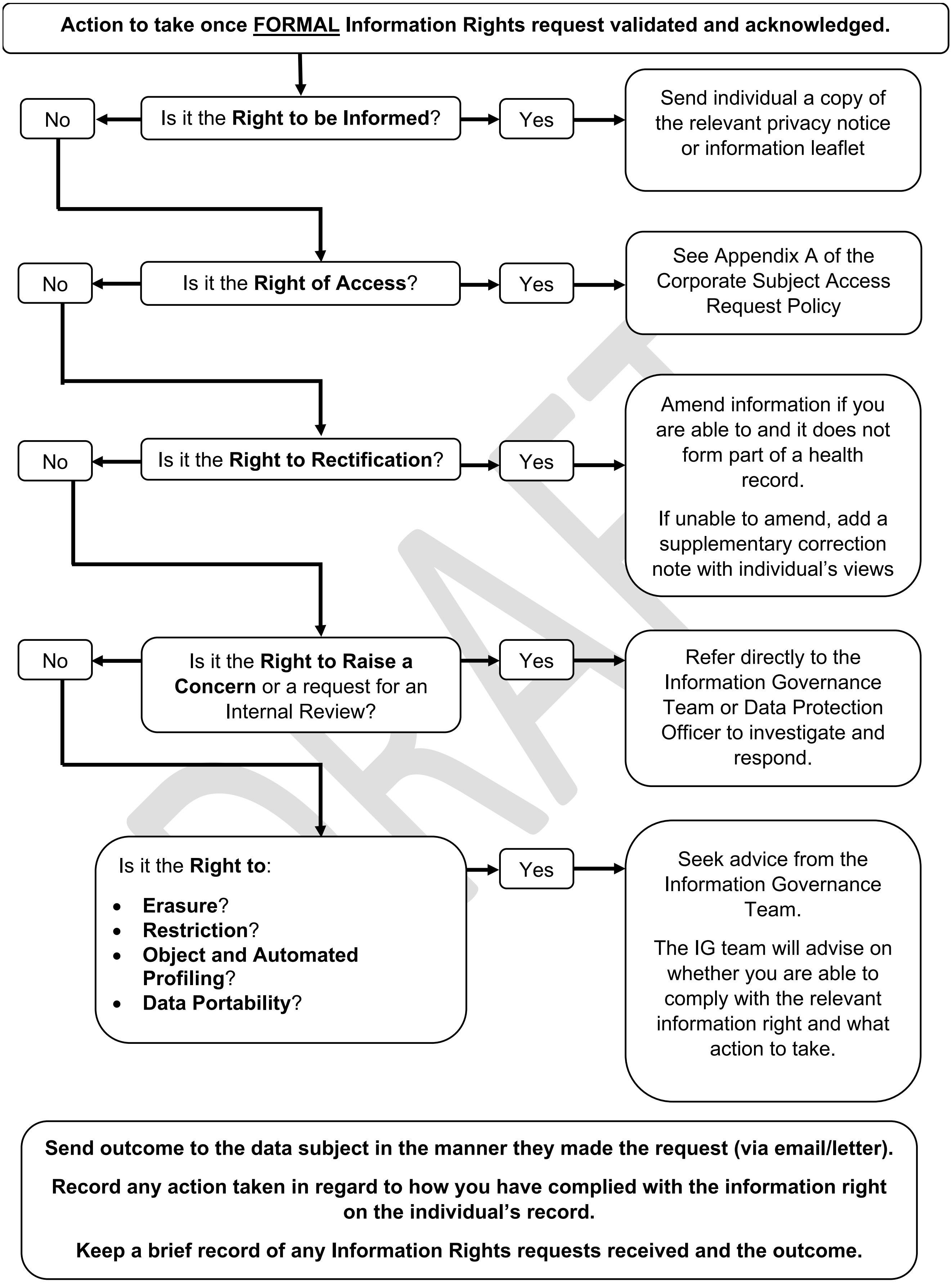
Confirmation sent to you with the outcome of your request

To Raise a Concern about our personal data processing or if you are dissatisfied with how your request has been handled, you can ask for an internal review.

- *To request an internal review you need to contact the Data Protection Officer, who is the Health Board lead on Data Protection via dpo.hdd@wales.nhs.uk*

If you are not satisfied following the outcome, you have the right to make a complaint to the ICO.

- *To make a complaint you need to contact the Information Commissioner, who is the statutory regulator*
- *You should raise your concerns within three months of your last contact with us*



Action to take once FORMAL Information Rights request validated and acknowledged.

Is it the **Right to be Informed**?

Yes → Send individual a copy of the relevant privacy notice or information leaflet

No

Is it the **Right of Access**?

Yes → See Appendix A of the Corporate Subject Access Request Policy

No

Is it the **Right to Rectification**?

Yes → Amend information if you are able to and it does not form part of a health record.

If unable to amend, add a supplementary correction note with individual's views

No

Is it the **Right to Raise a Concern** or a request for an Internal Review?

Yes → Refer directly to the Information Governance Team or Data Protection Officer to investigate and respond.

No

Is it the **Right to**:

- **Erasure**?
- **Restriction**?
- **Object and Automated Profiling**?
- **Data Portability**?

Yes → Seek advice from the Information Governance Team.

The IG team will advise on whether you are able to comply with the relevant information right and what action to take.

Send outcome to the data subject in the manner they made the request (via email/letter).

Record any action taken in regard to how you have complied with the information right on the individual's record.

Keep a brief record of any Information Rights requests received and the outcome.

UNAUTHORISED ACCESS TO PATIENT RECORDS - REPORTING AND ESCALATION PROCEDURE

Procedure information

Procedure number: **773**

Classification:
Corporate

Supersedes:
N/A

Version number:
1

Date of Equality Impact Assessment:
12/07/2022

Approval information

Approved by:
Sustainable Resources Committee

Date of approval:
Enter approval date
Date made active:
Enter date made active (completion by policy team)
Review date:
Enter review date (normally three years from approval date)

Summary of document:
This document includes the correct procedure for the use of the National Integrated Intelligence Audit Solution (NIIAS) to identify potentially inappropriate access to clinical records and how to escalate this through an agreed process.

Scope:
All staff with access to electronic clinical systems will be affected by the introduction of NIIAS. Staff within the Health Board have been fully briefed as to what this system will deliver through a robust communications plan, Information Governance training sessions and discussions at the relevant forums (including Staff Partnership Forum). Communication reminders are sent to staff on a regular basis to remind them of their responsibilities in relation to accessing patient records and respecting patient privacy and confidentiality.

To be read in conjunction with:
320 – Acceptable Use of IT Policy – opens in a new tab
172 – Confidentiality Policy– opens in a new tab
836 – All Wales Information Governance Policy – opens in a new tab
837 – All Wales Information Security Policy – opens in a new tab
995 - All Wales Respect and Resolution Policy – opens in a new tab
201 - All Wales Disciplinary Policy and Procedure – opens in a new tab
435 - All Wales NHS Staff to Raise Concerns Procedure (Whistleblowing) – opens in a new tab
488 - All Wales Upholding Professional Standards in Wales (Medical & Dental Staff) Policy – opens in a new tab

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub Committee
08/04/2023

Executive Director job title:
Huw Thomas , Director of Finance

Reviews and updates:
1.0 New Procedure

Keywords
NIIAS, Audit, Information Governance, Unauthorised Access

Glossary of terms

Term	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
Data Protection Legislation	Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.
NIIAS	National Integrated Intelligent Audit Solution
Personal Data	Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as patients or service users.
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Senior Information Risk Owner (SIRO)

An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board.

Special Category Data

Special category data means personal data consisting of information as to:

- Genetic and biometric data
- Political opinions
- Religious or other beliefs
- Trade union membership
- Physical or mental health/condition
- Sexual life

And although not specifically described as special category data, this information requires the same treatment:

- The commission or alleged commission of any offence
- Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings

Unauthorised Access

Access to information that is not part of your work duties. Access to a patients record where the patient is not under your care.

Contents

Scope

All staff with access to electronic clinical systems will be affected by the introduction of NIIAS. Staff within the Health Board have been fully briefed as to what this system will deliver through a robust communications plan, Information Governance training sessions and discussions at the relevant forums (including Staff Partnership Forum). Communication reminders are sent to staff on a regular basis to remind them of their responsibilities in relation to accessing patient records and respecting patient privacy and confidentiality.

Aim

The aim of this document is to:

- ensure appropriate and relevant access to Patient Identifiable Information (PII).
- ensure that all staff understand their responsibilities when accessing patient records.
- educate staff on the process Information Governance will take on any identified inappropriate access to information.
- ensure the Health Board has taken all steps possible to educate staff to prevent any future breaches of confidentiality.

Objectives

The aim of this document will be achieved by the following objectives:

- Identify any potential inappropriate access to PII in line with the principles of the current Data Protection Legislation and confidentiality and privacy laws to ensure that patient information is handled by staff members fully respecting the privacy rights of each individual patient.
- Escalate any potential Personal Data Beaches to the Information Governance team so that action can be taken.
- Where a case has to be answered, inform the Workforce Department to follow the processes outlined within this procedure and which may result in action being taken in line with the Health Board's Disciplinary Policy and Procedure – opens in a new tab.

Introduction

The National Intelligent Integrated Audit Solution (NIIAS) will take the audit trail from electronic clinical systems, e.g. Welsh Patient Administration System (WPAS), Laboratory Information Management System (LIMS), the Welsh Clinical Portal (WCP) and cross match against both an employee record in the Electronic Staff Record (ESR) and the Health Board's national directory (Cymru). NIIAS will then report on any unauthorised access to person identifiable information (PII) against the domains outlined in section 2.1.

Procedure

The Procedures follow several steps to identify and escalate potential personal data breaches:

Definition of the 8 domains

Breaches have been defined on a National level and fall into the following 8 domains.

Term	Definition	Comment
Own Care Record	A user has accessed their own patient records.	Identification of Patient IDs for the staff member through ESR-MPI triangulation.
Family Care Record	A User has accessed the record of a Patient who has the same surname and postcode as the User.	Family classified as matching same surname + postcode through ESR-MPI triangulation.
Staff Member Record	A User has accessed the record of a Patient who has a matching employee record in ESR.	
Living in the Same Vicinity	A User has accessed the record of a Patient who lives very close to the User. In rural areas this distance is 0.5 miles, in urban areas this distance is 0.1 miles.	Identification of distance between User and Patient postcodes through ESR-MPI triangulation.
Person of Interest	A User has accessed the record of a Patient who has been flagged by the HBs as being a “person of interest”.	This Patient is flagged locally using their NHS number.
Patients with the Same Surname	A User has accessed three Patients in the space of 1 day who share the same surname.	The 15 most common surnames in Wales have been excluded (Davies, Edwards, Evans, Griffiths, Hughes, James, Jenkins, Jones, Lewis, Morgan, Rees, Roberts, Smith, Thomas, and Williams).
Historic Record	A User has accessed patient records that are older than 1 year without first accessing a more recent record for that same Patient within the last 45 days.	Users with Clinical Job Roles assigned in ESR are excluded.
Deceased Patient	A User has accessed the records of a deceased Patient who has been deceased for more than 60 days.	Identification of deceased patient through MPI.

The Health Board is currently enforcing the following domains:

- Access to Own Record;
- Access to Family Record;
- Access to Persons of Interest;
- Access to Deceased patient's records; and
- Access to Staff Members Records.

Process for managing Access to Own Record: First time accessed by staff member (See Appendix 1 for flow chart)

The Information Governance team will produce a daily report that will identify any staff accesses to own record. Any staff member identified through the report will be sent an e-mail with an attached letter from the Information Governance Team outlining the details of the access. The attached letter will advise staff that they need to share a copy of the letter with their line manager within 5 working days, and attend one of the Information Governance Awareness Training sessions. Individuals are advised that attendance at the training session will be recorded on their ESR record.

Line Managers are then requested to confirm receipt of the letter to the Information Governance Team within 10 working days by completing the attached FORM 1 and confirming which of the Information Governance Awareness training sessions the individual will attend.

Staff will then book via ESR or directly with IG onto a virtual training session of their choosing.

Following completion of the training, any further attempts by a staff member to access their Own Record within a two-year period will be dealt with formally through the NIIAS procedure for further access to own record (see point below).

NB: If at any point during the analysis of the NIIAS report the Information Governance Team, Executive Lead or Manager suspects there has been serious malpractice carried out by an employee a full investigation can be undertaken.

If a member of staff fails to respond to the Information Governance team, manager details are requested via Workforce.

Process for managing Access to Own Record: Further access by staff member (See Appendix 2 for flow chart)

The line manager for the staff in question will be contacted and asked to complete an 'Initial Assessment of Facts Form'. This will be returned to the Information Governance Team within 10 working days.

If it is not possible to identify the line manager for the staff member in question, the process outlined in the point above will be followed to make initial contact with the staff member and to request details of their line manager.

The Information Governance Team will review the returned 'Initial Assessment of Facts Form'. If the access is deemed as appropriate by the line manager (i.e. there is a legitimate work reason for the staff member accessing the record) and this is confirmed and agreed by the Information Governance team, the case will be closed on the NIIAS tracker and no further action taken.

If the access was inappropriate, the Information Governance Team will send details of the access and the outcome of the returned 'Initial Assessments of Facts Form' and investigation through to the identified link in the Workforce team to initiate the procedure as detailed in the All Wales Disciplinary Policy and Procedure document – opens in a new tab.

The Workforce team will liaise with the line manager to agree any further action required in relation to the staff member.

The Information Governance Team will provide any appropriate NIIAS reports as requested by the Workforce team.

Process for managing access to Family Record, Staff Record, Persons of Interest and Deceased patient's records. (See Appendix 3 for flow chart)

The Information Governance team will produce a report daily that will identify any staff accesses to the records above.

The individual staff member will be sent an e-mail with an attached basic letter advising them they have been identified through the NIIAS system as potentially having accessed a record without authorisation to do so. Staff will be asked to enter details of their line manager onto the contact letter and return this to the Information Governance team within 5 working days.

The Information Governance team will then contact the line manager directly with full details of the breach and ask that they complete an 'Initial Assessment of Facts Form' to identify whether the access is appropriate or not in relation to their staff member. This form will then be returned to the Information Governance team within 10 working days.

Appropriate access to records of Family Member, Staff Record, Persons of Interest and Deceased patient's records.

If the breach is deemed as appropriate by the line manager (i.e. there is a legitimate work reason for the staff member accessing the record) and this is confirmed and agreed by the Information Governance team, the case will be closed on the NIIAS tracker and no further action taken.

Inappropriate access to record of Family Member, Staff Record, Persons of Interest and Deceased patient's records.

The line manager will be required to conduct a formal meeting with the staff member to advise them that their access to the record is not appropriate, remind them of the NIIAS procedure and the Health Board's Confidentiality Policy – opens in a new tab. The line manager may wish to link in with their HR advisor within the Workforce team to assist with this process if further support is required.

The IG Team will run a full NIIAS check report against the individual to ensure there are no wider concerns about the individual's access to patient records.

The staff member will be required to attend an Information Governance training session within three months. The NIIAS tracker will be updated once the staff member has completed their IG training and the IG Team have completed their report. If no further inappropriate access to records takes place and no wider concerns are identified, then no further action will be taken and the case will be considered for closure.

If the access relates to more than a single record access or, if there are wider concerns confirmed or noticed about the individual's access to records, the Information Governance Team will commence the procedure for Managing Information Governance Incidents. This will be run alongside any on-going disciplinary/Workforce investigation. The Information Governance and Workforce teams will share information from their on-going investigations where it is felt appropriate to do so.

As part of the Managing Information Governance Incidents Procedure, the Information Governance Team will report the breach to the Caldicott Guardian and Senior Information Risk Owner who may decide to immediately suspend the staff member's access to patient records whilst the investigation is on-going. The Information Governance team will also need to determine if the breach is reportable to the Information Commissioner Office, this is in accordance with the Health Boards statutory obligations to report personal data breaches.

Once the investigation has concluded the Information Governance team will be informed by the Workforce link

NB: If at any point during the analysis of the NIIAS report the Information Governance team, Executive Lead or Manager suspect there has been serious malpractice carried out by an employee i.e. evidence that a large number of records have been accessed or multiple family members etc, this should be reported immediately to the Head of Information Governance and the Director of Digital Services.

Escalation process for all non-responses from staff and managers

If an individual member or line manager do not respond to requests for information from the Information Governance team within the agreed time-scales at any stage of the NIIAS process, the following action will be taken:

- An initial chaser e-mail will be sent by the Information Governance Team requesting a response within 5 working days.
- If no response, then the Workforce will be contacted for the employees managers details. If the manager fails to respond their line manager will be contacted.
- If no response received details will be sent to the relevant Executive Director who will contact the line manager requesting a response within 10 working days be sent to the Information Governance team.

Escalation process for not attending a booked Information Governance training session (without giving prior notice to the IG Team)

- An e-mail will be sent to the individual's line manager advising their staff member did not attend the IG training session. The line manager will be requested to remind the individual to book onto another IG training session and to respond within 5 working days.
- If no response then a second chaser e-mail will be sent requesting a response within a further 5 working days.
- If the individual does not attend the re-booked IG training session that their line manager has confirmed, they will be referred to their Executive Director with a request that they attend the next training session available, and their line manager will be copied into this e-mail.
- If the line manager does not respond to any requests to re-book their staff member onto a future session by the IG team then they will be referred to their Executive Director and a response will formally be requested.

Choose Pharmacy Application

The Choose Pharmacy application supports the delivery of a number of NHS community pharmacy services and enables access to NHS patient record systems including the Welsh Demographic Service and the Welsh GP Record.

The Health Board will be responsible for monitoring community pharmacy staff's access to patient data through the above application via the NIIAS monitoring tool.

The NIIAS system provides a report of potential breaches, this is then analysed by the Information Governance team on a twice weekly basis.

The Information Governance Team will then e-mail a report of any potential breaches to the Primary Care Manager (Community Pharmacy).

The Primary Care Manager will then contact the relevant pharmacy and ask that the following process is completed:

Pharmacy staff accessing their own record on one occasion (See Appendix 4 for flow chart)

The Pharmacist must issue a warning email for staff members accessing their own record on the first occasion. They must confirm that this action has been completed to the Primary Care Manager. The Primary Care Manager will then inform the Information Governance Team that this action has been taken.

Where the access has been made by the pharmacy superintendent/pharmacy owner, the Primary Care Manager will send the warning email.

Pharmacy staff accessing their own record on more than one occasion or potentially accessing another person's record inappropriately (See Appendix 5 for flow chart)

The Primary Care Manager will request that the Pharmacist undertake an initial assessment using the Potential Access Breach – Initial Assessment Form to establish whether there is a legitimate clinical or administrative reason for the staff member to have accessed the record(s) for second access to own record or all other potential breaches.

The potential breach will be communicated to the superintendent pharmacist for the community pharmacy at which the breach occurred. The superintendent will provide the Primary Care Manager with the name of the person who will undertake the initial assessment within 5 days.

The initial assessment must be undertaken within 10 working days from a date agreed between the superintendent/owner and the Health Board.

The outcome of the initial assessment should be communicated to the Primary Care Manager via the Potential Access Breach – Initial Assessment Form.

Where the assessment concludes that no further action is necessary the Primary Care Manager will confirm they are satisfied with this decision. The Primary Care Manager will inform the Information Governance Team that no further action is required.

Where the assessment indicates the need for a full investigation – this should be completed in line with the pharmacy Information Governance policy for the management of Information Governance incidents. Access to the Choose Pharmacy application may be removed for the duration of the investigation. The outcome of the investigation will be reported to the Primary Care Manager who will inform the Information Governance Team that the record can be closed.

Any further general learning or training identified following the investigation will be agreed between the Primary Care Manager and the Information Governance team and progress monitored through the Information Governance tracker.

If the inappropriate access is carried out by the Pharmacy Owner/superintendent pharmacist then the Primary Care Manager will appoint an appropriate individual within the Health Board to carry out a full investigation.

Training

All staff will be required to have appropriate Information Governance training, additional training can be requested by individuals or line managers. Training will be provided in several formats to accommodate all learning styles and the requirements of staff and The Health Board.

Implementation

Extensive communications exercises have been undertaken to ensure all staff groups are aware of NIIAS and the implications of any breaches identified. This will be further supported through Information Governance communications via Globals / Newsletters / IG Awareness on Intranet.

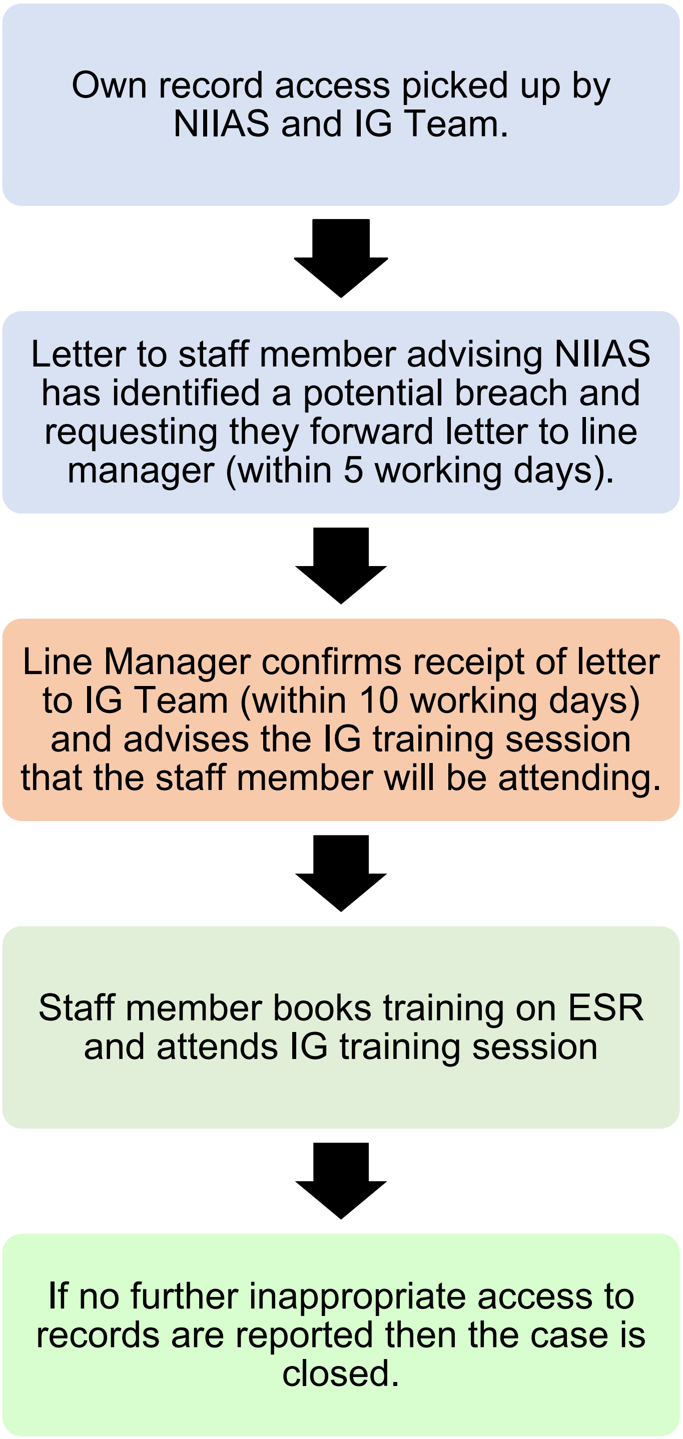
Review

This Procedure will be reviewed in line with the further roll out and enforcement of the policy rules, or sooner, as required.

References

Information Commissioner Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Appendix 1 – Process for managing Access to Own Record: First access by staff member



Own record access picked up by NIIAS and IG Team.

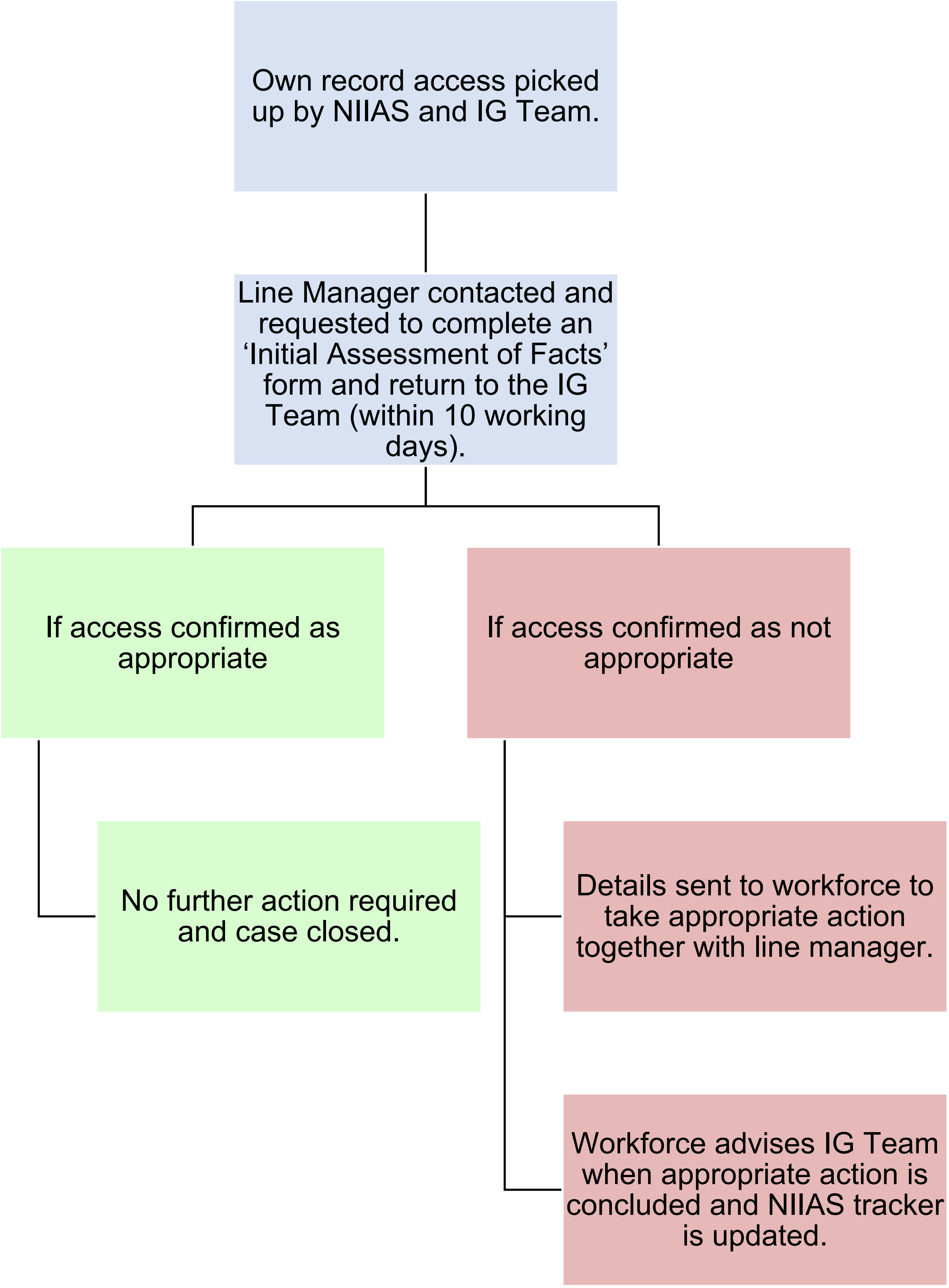
Letter to staff member advising NIIAS has identified a potential breach and requesting they forward letter to line manager (within 5 working days).

Line Manager confirms receipt of letter to IG Team (within 10 working days) and advises the IG training session that the staff member will be attending.

Staff member books training on ESR and attends IG training session

If no further inappropriate access to records are reported then the case is closed.

Appendix 2 – Process for managing Access to Own Record: Further access by staff member



Own record access picked up by NIIAS and IG Team.

Line Manager contacted and requested to complete an ‘Initial Assessment of Facts’ form and return to the IG Team (within 10 working days).

If access confirmed as appropriate

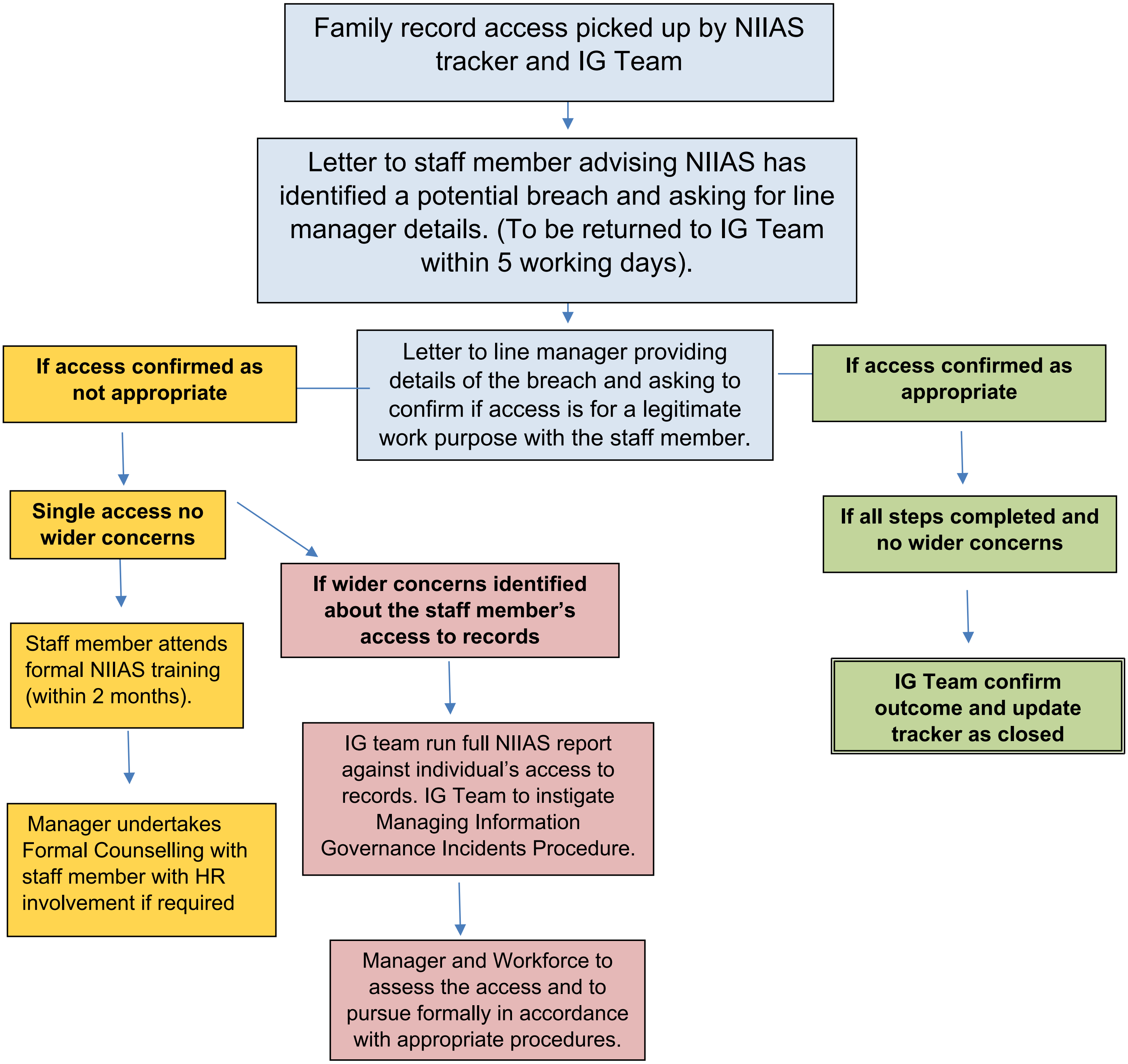
No further action required and case closed.

If access confirmed as not appropriate

Details sent to workforce to take appropriate action together with line manager.

Workforce advises IG Team when appropriate action is concluded and NIIAS tracker is updated.

Appendix 3 - Process for managing access to Family Record, Staff Record, Persons of Interest and Deceased patient's records.



Family record access picked up by NIIAS tracker and IG Team

Letter to staff member advising NIIAS has identified a potential breach and asking for line manager details. (To be returned to IG Team within 5 working days).

Letter to line manager providing details of the breach and asking to confirm if access is for a legitimate work purpose with the staff member.

If access confirmed as not appropriate

Single access no wider concerns

Staff member attends formal NIIAS training (within 2 months).

Manager undertakes Formal Counselling with staff member with HR involvement if required

If wider concerns identified about the staff member's access to records

IG team run full NIIAS report against individual's access to records. IG Team to instigate Managing Information Governance Incidents Procedure.

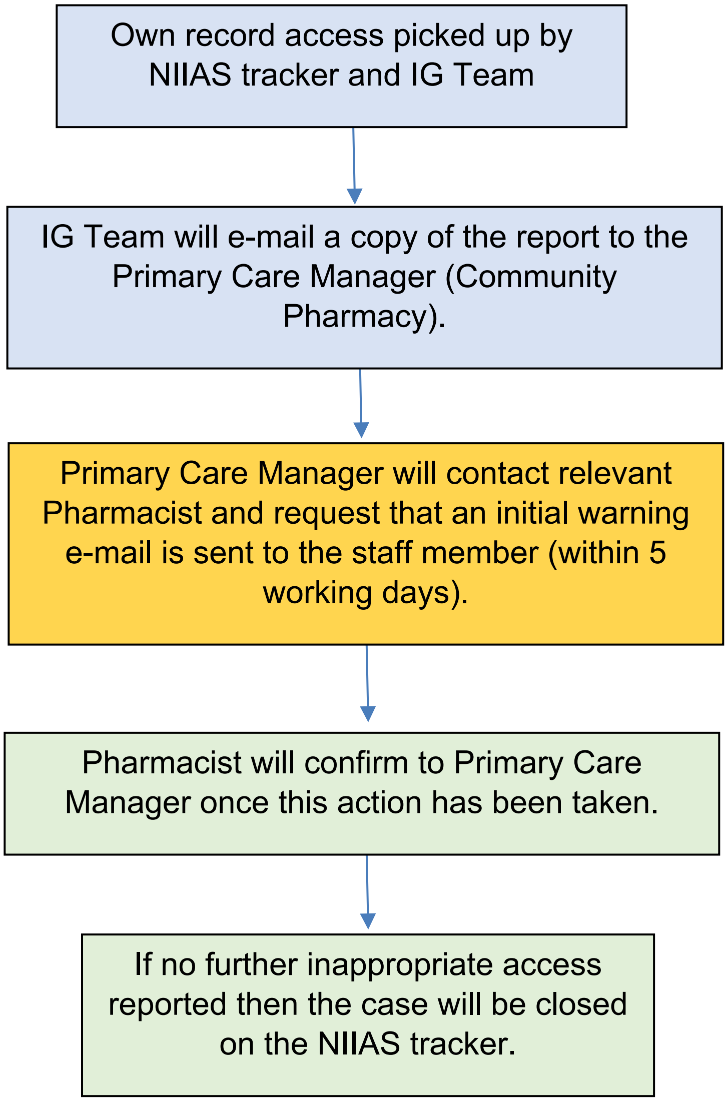
Manager and Workforce to assess the access and to pursue formally in accordance with appropriate procedures.

If access confirmed as appropriate

If all steps completed and no wider concerns

IG Team confirm outcome and update tracker as closed

Appendix 4: Pharmacy staff accessing their own record on one occasion



Own record access picked up by NIIAS tracker and IG Team

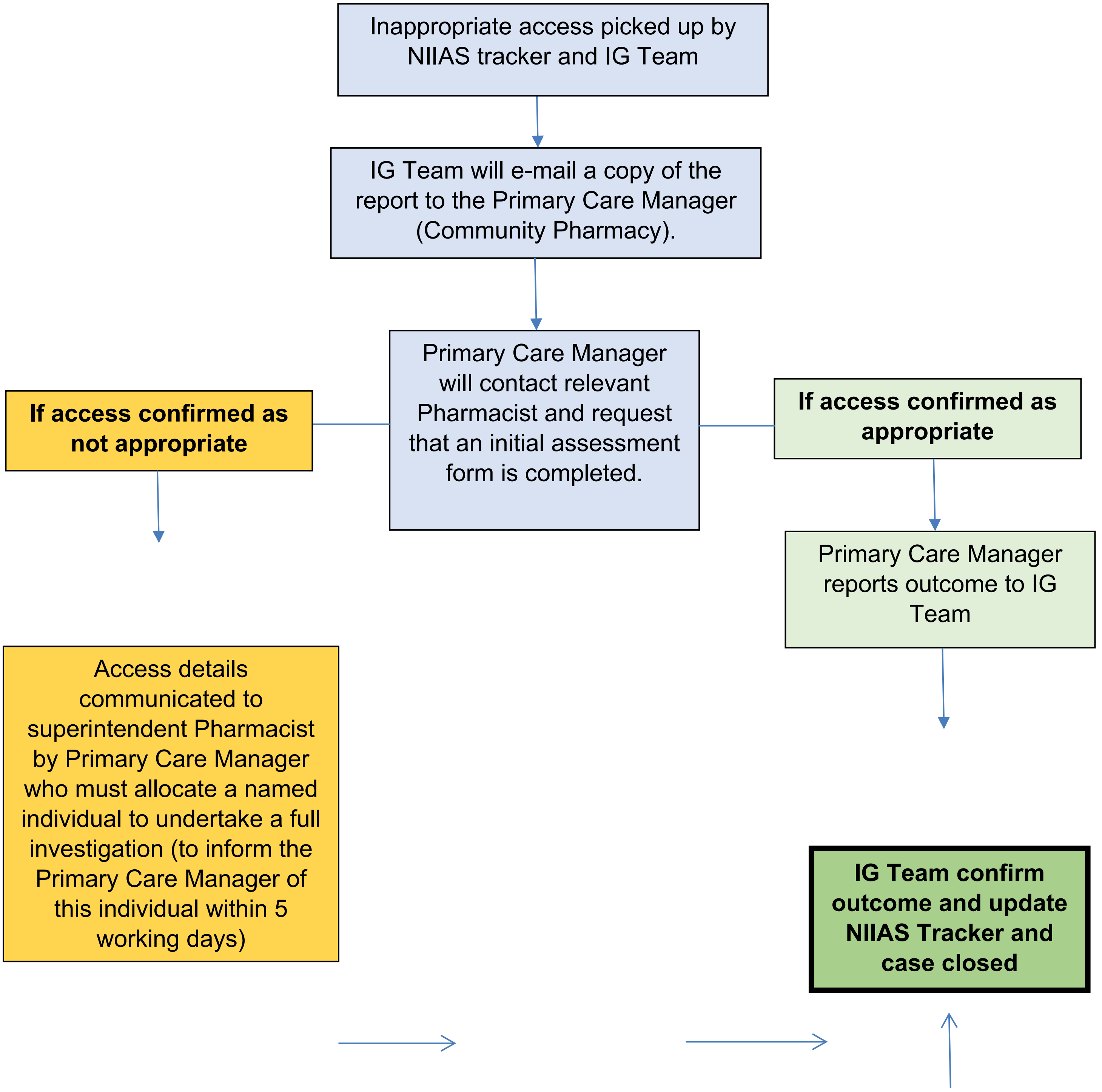
IG Team will e-mail a copy of the report to the Primary Care Manager (Community Pharmacy).

Primary Care Manager will contact relevant Pharmacist and request that an initial warning e-mail is sent to the staff member (within 5 working days).

Pharmacist will confirm to Primary Care Manager once this action has been taken.

If no further inappropriate access reported then the case will be closed on the NIIAS tracker.

Appendix 5: Pharmacy staff accessing their own record on more than one occasion or potentially accessing another person’s record inappropriately



Inappropriate access picked up by NIIAS tracker and IG Team

IG Team will e-mail a copy of the report to the Primary Care Manager (Community Pharmacy).

Primary Care Manager will contact relevant Pharmacist and request that an initial assessment form is completed.

If access confirmed as not appropriate

Access details communicated to superintendent Pharmacist by Primary Care Manager who must allocate a named individual to undertake a full investigation (to inform the Primary Care Manager of this individual within 5 working days)

If access confirmed as appropriate

Primary Care Manager reports outcome to IG Team

IG Team confirm outcome and update NIIAS Tracker and case closed

Full investigation undertaken in line with the Pharmacy's Information Governance Policy for the management of information governance incidents/breaches of confidentiality.

Outcome of investigation is reported to the Primary Care Manager by the superintendent Pharmacist.

Primary Care Manager advises the IG Team once the investigation has concluded.