NHS
Kernow
Clinical Commissioning Group

Information Governance Handbook
Management Guidance Notes

Corporate Governance Team

Version number	Effective date	Changes (By whom and why)
1.0	Dec 18	Initial Version being developed by Trudy Corsellis and Jodeigh Phelps
1.1	Feb 19	Updated for change to IG breach reporting template

NHS
Kernow
Clinical Commissioning Group

Contents

1. Introduction to Information Governance

Information governance is the way in which an organisation governs the information it holds, this includes:

- Data Protection
- Confidentiality
- Corporate information
- Information and cyber security
- Records Management
- Data Quality

Information is a vital asset, both in terms of the clinical management of individuals and the efficient commissioning and management of services and resources. Therefore it is essential that NHS Kernow ensures its information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically, and
- Shared appropriately and lawfully
- Arrangements for secure disposal

How this guidance will help you

This guidance provides staff with information on a range of issues relating to information governance to assist staff in being compliant with the relevant legislation and local policies. The aim of this booklet is to ensure that you are aware of your roles and responsibilities for Information Governance.

Please remember the principles and requirements surrounding data protection and confidentiality extend to more than just patient records. Personal data is also contained with staff personnel files and is therefore covered by the Data Protection Act 2018. In addition, many aspects of the CCG's work is confidential and so should not be disclosed without prior approval, e.g. contracting and procurement information, accounting and invoicing information, part 2 minutes of meetings, etc.

Also, as can be seen from the records retention section, it is also important that NHS Kernow retains specific information for certain lengths of time as there are statutory duties the CCG is expected to comply with. Staff help and support with this is much appreciated.

Information governance is everyone's responsibility

2. Data Security and Awareness Overview

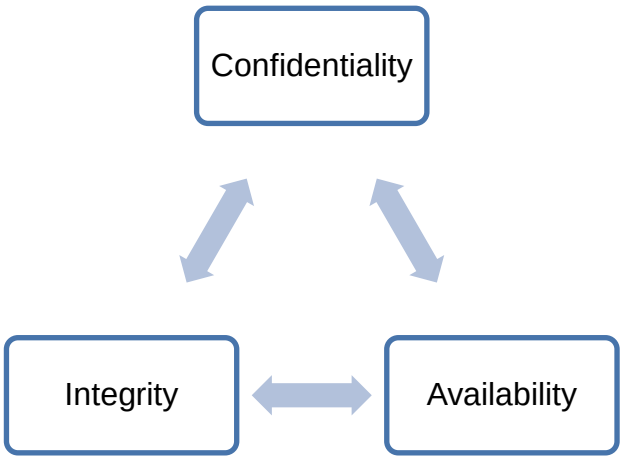
The National Data Guardian (NDG) Review requires that all NHS staff undertake appropriate annual data security training and pass a mandatory test. This also includes non-permanent staff that have access to personal confidential information.

Data Security has always been important. In fact, it's no more important today than it's always been. But it's become more complex and time-consuming to manage now that technology is so central to the way we deliver health and care.
These technologies provide fantastic opportunities. By and large, technology is designed for safe and effective use. But, as an organisation, we must ensure that we use it in a way that does not pose unacceptable risk to our business or the people in our care.

We all have a duty to protect people's information in a safe and secure manner.

Confidentiality, Integrity, Availability

Data Security can be broken down into three areas: Confidentiality, Integrity & Availability.



Confidentiality is about privacy and ensuring information is only accessible to those with a proven need to see it.

It would be unacceptable for a perfect stranger to be able to access sensitive information from a laptop simply by lifting the lid and switching it on. That's why a laptop should be password-protected and the data on it encrypted when switched off.

Integrity is about information stored in a database being consistent and un-modified.

Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration.

Availability is about information being there when it's needed to support care.

System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct and can be relied on when providing health or care.

Help and Support available

If you are unsure about an information governance issue please speak to your line manager. Additionally, the Corporate Governance team, the Head of Information Governance and/or the Data Protection officer are here to help and advise.

3. Key Information Governance Roles

A number of key Information Governance related roles exist which you need to be aware of.

Senior Information Risk Owner (SIRO)

The SIRO is responsible for, and takes ownership of, NHS Kernow's risk policy and all aspects of risk associated with information governance, including those relating to confidentiality and data protection. The SIRO is the board level lead for information risk. NHS Kernow's SIRO is Helen Childs.

Caldicott Guardian

The Caldicott Guardian is responsible for, and takes ownership of, ensuring that NHS Kernow satisfies the highest practical standards for handling patient identifiable information. Any sharing of identifiable data should be reviewed by the Caldicott Guardian first. NHS Kernow's Caldicott Guardian is Natalie Jones

Data Protection Officer (DPO)

NHS Kernow's DPO is Trudy Corsellis. The Data Protection Officer offers expert knowledge of data protection law and practices. These are:

- to inform and advise NHS Kernow and its employees about their obligations to comply with the General Data Protection Regulation (GDPR) and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including assigning responsibilities, managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to cooperate with the Information Commissioner's Office (ICO)

- to act as the contact point for the ICO and for individuals whose data is processed (employees, patients etc.).

Under GDPR, the role of DPO is protected and NHS Kernow must ensure that:

- The DPO reports to the highest management level of NHS Kernow – i.e. Governing Body level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Information Asset Owners (IAOs)

The Information Asset Owner is a senior manager who takes responsibility for the security of information of a specific information system or systems within NHS Kernow, as well as understanding and taking ownership of the risks relating to NHS Kernow's assets and to provide assurance to the SIRO.

Information Asset Administrators (IAAs)

The Information Asset Administrator is responsible for the day to day running of one or more information systems and for ensuring that policies and procedure are adhered to, bringing any actual and/or potential risks to the attention of the IAOs.

4. Information Governance Policies

The purpose of the Information Governance (IG) Strategy is to set out NHS Kernow's IG framework and associated priorities in order that appropriate processes and controls are put in place to protect the CCG's information assets from all threats, whether internal or external, deliberate or accidental.

In addition to the IG Strategy, there are several IG and data protection related policies available on the document library. These include, but are not restricted to:

- Information Governance Policy
- Data Protection Policy
- Records Management Code of Practice
- Pseudonymisation Policy
- IT Security Policy and all linked policies
- Integrated Identity Management Policy
- Email Policy
- Safe Haven Policy

- Data Quality Policy
- Confidentiality Code of Conduct for Employees

The policies and procedures that were produced to support IG apply to NHS Kernow and all its employees, executive and non-executive staff, agency staff, seconded staff and contractors. The policies and procedures are reviewed on a regular basis in accordance with the requirements of the Data Security and Protection Toolkit or upon significant internal/external changes and in conjunction with annual security audits.

It is the responsibility of each member of staff to adhere to the policy and underpinning procedures.

5. What is Personal Data

Personal Data Personal data refers to all items of information in any format from which an individual might be identified or which could be combined with other available information to identify an individual. This includes (but is not limited to):

- Name
- Date of birth
- Postcode
- Address
- Online identities (usernames, IP addresses) and/or location (GPS) data
- Photographs, digital images etc.
- NHS number
- Date of death
- Pseudonymised data

If you are unsure if you are handling personal data there is a flowchart in appendix 2 which may be of assistance.

Special Categories of Personal Data Certain categories of information are classified as sensitive and additional safeguards are necessary when sharing or disclosing this information in line with guidance and legislation. This includes:

- Physical and mental health
- Genetic data
- Biometric data
- Social care
- Ethnicity and race
- Sexuality
- Trade union membership
- Political affiliations
- Religion

Records relating to criminal charges and offences are also to be treated as a special personal data.

NHS Kernow places great emphasis on the need for the strictest confidentiality in respect of personal confidential data and especially when using special category data. This applies to manual and computer records and conversations about individuals. Everyone working for NHS Kernow is under a contractual and legal duty to keep personal information, held in whatever form, confidential. Individuals who feel their confidentiality has been breached may raise a complaint under the complaints or grievance (for staff) procedure.

All organisations carrying out functions as part of, or on behalf of, the NHS have a contractual requirement to maintain the confidence to those whose information they process.

Your responsibilities to comply with the Common Law Duty of Confidentiality

All employees working in or on behalf of the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of contractual responsibilities but also a requirement within the common law duty of confidentiality, the Data Protection Act and the General Data Protection Regulation. It is also a requirement within the NHS Care Record Guarantee and NHS Constitution, produced to assure individuals regarding the use of their information.

A duty of confidence when handling privileged information is upheld by common law, statute, contract of employment, disciplinary codes and policies and professional registration. Additionally, corporate information may be considered sensitive, such as those relating to contract tenders.

This means staff need to consider whether they are sharing confidential information appropriately. There are some easy steps to take:

- Do not forward personal data to a long list of email recipients without considering if everybody needs to have the personal information
- Do not discuss cases you are involved with unnecessarily, this includes inside and outside of the organisation, particularly bear in mind having conversations about individuals in open communal areas such as coffee areas and car parks

Where personal confidential or otherwise sensitive data is held then NHS Kernow needs to take appropriate measures to ensure that it is secure and confidential.
If there is no ongoing need to retain data in an identifiable form, then it should be pseudonymised/ anonymised as soon as possible to reduce risk of inappropriate retention, disclosure or loss.

Please refer to records retention periods for more details on records management.

6. Managing emails – tips and reminders

Emails form part of the formal records of NHS Kernow and are governed by NHS records management policy.

Please remember that emails should be used as a form of communication only and not as a filing system for information that belongs to our service users and staff or has value to the organisation.

(i) Emails should be saved as part of a formal record and not kept in your inbox
If you make a decision and then leave the organisation the decisions you have made on behalf of the organisation need to be obtainable, therefore please make sure you are saving emails appropriately. It is imperative the email and/or attachment is saved in the appropriate place, be this a shared drive or a p-file for a member of staff.

(ii) Emails should not be kept in inboxes 'just in case'
As described above, emails should be retained as part of a proper record where appropriate or deleted. There should be nothing in your personal inbox for more than 6 months, this allows for the correct storage of corporate and personal information. It also means that if an individual makes a subject access request the organisation knows where to locate this information.

(iii) Check the addressee(s)
Many accidental breaches are made when emails are sent to the wrong recipient. Please double check before you press send.

(iv) Think before you hit reply all or forward
Do all the people you are emailing need to receive the email? Is the information in the email personal and therefore should not be sent to everyone on the distribution list. Also, do not automatically assume the originating emailer had the correct email addresses.

(v) Think – do you need to send an email?
If you want to discuss something personal or confidential first consider if you could pick up the phone or go and speak to the other individual about your concerns, just because an item is out of your inbox does not mean the other person has dealt with it or deleted it if you think it needs deleting.

(vi) Archive
Do not save to the email archive as this creates a permanent record which can only be deleted by CITS. It is a record that the organisation will have to access if a subject access request or freedom of information request is made.

(vii) Out office
Do use an out of office message to advise when you are not available and provide a point of contact during the absence.

(viii) Be aware
Your mailbox may be accessed if you are absent, e.g. sickness on holiday.

7. Data protection by design and default

Data Protection by Design and Default is now a legal requirement. The Data Protection Act 2018 requires NHS Kernow to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'.

Privacy by design is based on seven "foundational principles"

- Proactive not reactive; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

In essence, this means NHS Kernow staff have to integrate data protection into processing activities and business practices, from the design stage right through its lifecycle. The concept is not new and was previously known as 'privacy by design' but, as noted above, it is now a legal requirement.

"Data protection by design" refers to:

- Developing organisational policies, business practices, strategies with privacy implications
- Physical design – visibility, transparency, audit trails, use of pseudonymisation and safeguards
- Embarking on new data sharing initiatives
- Using personal data for new purposes

"Data protection by default" requires organisations to ensure they only process the data that is necessary to achieve their specific purpose. It must have regard for data minimisation and purpose limitation principles and should:

- Specify data requirements before processing starts
- Appropriately inform individuals - do not just provide an illusory choice
- Do not process additional data unless individuals say you can

- Ensure data is not automatically made publicly available to others unless individuals decides to make it
- Provide individuals with sufficient controls and options to exercise their rights

Therefore it is imperative that when you are thinking about starting a new process or project you consider data protection ask yourself:

- What personal information do I need to complete the work?
- Who will the information be shared with?
- Who will have access to the information and how long do we need to/should we keep it?
- Do I have a legal basis for collecting, storing and sharing the information?
- How do we pseudonymised as much of the information as possible?
- Have I completed a Data Protection Impact Assessment?
- Have I sought advice from the Corporate Governance team?

The Head of Information Governance and/or the Data Protection Officer are here to help you work through any issues to enable you to carry out the work you are required to do. Completing a Data Protection Impact Assessment (DPIA) will help you work through these issues.

8. Data protection impact assessment

NHS Kernow **must** complete a DPIA when:

- Processing involves using new technologies
- Processing is likely to result in a high risk to the rights and freedoms of individuals
- Systematic and extensive evaluation of personal characteristics based on automated decision making processes, including profiling, where decision have legal effects or significantly affect them
- Processing on a large scale of special category data
- Large systematic monitoring of public areas (CCTV)

The above list is frequently deemed to be the “high risk” areas.

The DPIA process helps identify and minimise data protection risks. It is essential that the DPIA:

i. Covers the following essential areas:
    - Describes the nature, scope, context and purposes of processing
    - Assesses necessity, proportionality and compliance
    - Identifies and assesses risks to individuals
    - Identifies any additional measures to mitigate risks

ii. Assesses risks in terms of both likelihood and severity
iii. Secures the input and advice of the Data Protection Officer as well as individuals and experts plus processors, where appropriate
iv. Mitigates risks and if high risk cannot be mitigated the ICO must be consulted before starting processing – they will give written advice within 8 weeks, 14 if complex
v. Is revised and updated it there is a change to nature, scope, context or purposes of processing

If no DPIA is completed, the reasons will need to be documented and recorded by the Corporate Governance team.

For those areas not considered "high risk", it is still considered good practice to complete a DPIA for other major projects and in the following instances:

- Evaluation or scoring
- Systematic monitoring / extensive profiling or automated decision making processes
- Processing special category or sensitive data incl. children, biometrics or genetics, criminal offences
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use or applying technological org solutions
- Data transferred outside the EU
- Processing data when not providing privacy notice directly to individuals
- Processing data which could result in risk of physical harm in the event of a security breach
- Processing which involves tracking on-line behaviour

NHS Kernow uses two different DPIA templates. The Comprehensive DPIA template is likely to be used only in exceptional circumstances (see **Appendix 1b**) which are deemed to have high risks that cannot be mitigated. It is envisaged the Simple DPIA template will typically be used - see **Appendix 1a.** Once completed, both templates should be sent to kccg.corporategovernance@nhs.net for advice and approval. This will then be signed and added to the Information Flows Register. This proforma has been designed to support staff to work within the law when considering the use of any personal data.

Once completed and signed off, all DPIAs will be logged on NHS Kernow's Information Flows Register. They are expected to be reviewed by the IAO in accordance with the timescale indicated within each document or sooner should nature, scope, context or purposes of processing change or a breach occur.

If a DPIA identifies a high risk which cannot be mitigated, the Data Protection Officer must be contacted. No processing of the information can take place before the ICO has been consulted and responded to NHS Kernow formally. The ICO endeavours to respond to all such contact within 8 weeks.

Appendix 1c provides the answers to a list of frequently asked questions relating to DPIAs.

9. Individuals' rights under the Data Protection Act

Under the Data Protection Act 2018, every individual has the following rights with respect to the personal data the CCG holds. This includes NHS Kernow staff and how the CCG uses their information.

a) **The right to be informed:** this includes how are we use their data, why, for what purpose, who are we sharing it with, how long will we keep it for, etc.

b) **Right of access**: this includes subject access requests (see below) and enables an individual to see all the information NHS Kernow holds on them.

c) **Right of rectification**: it is essential the information NHS Kernow holds is accurate. If an individual asks for information to be corrected or rectified to due errors, the CCG has 30 days to make the amendments. Should it opt not to, it must explain its reasoning to the individual who then has a right to complaint to the Information Commissioners Office (ICO).

d) **Right to erasure**: an individual can, under certain circumstances request that their information is deleted from systems, for examples when:
- personal data is no longer necessary for which it was originally collected
- the individual withdraws consent which was deemed the legal basis
- personal data has been unlawfully processed
- personal data has been erased for compliance with a legal obligation

Before doing so an assessment is needed on whether this is appropriate and the rationale needs documenting.

e) **Right to restrict processing**: an individual may be entitled to ask NHS Kernow to stop using (processing) their information. Examples could be when:
- the accuracy of personal data is contested
- the processing is unlawful, but the individual opposes erasure and requests restriction instead
- NHS Kernow no longer needs the personal data but is required to retain it for the exercise, establishment or defence of legal claim
- the individual has objected to processing based on using the public test or legitimate interest as the legal basis, as opposed to securing their consent

Whilst establishing whether the individual is correct in their right to restrict processing, NHS Kernow should refrain from using the individual's personal data until a decision is made. Once again, the CCG has a maximum of 30 days to do this.

f) **Right to data portability**: this is not to do with the portability of health records. It relates to the ability to switch easily between providers that offer IT enabled services using commonly- used and machine-readable format, that tracks and records data through an automated means, e.g. Fitbit

g) **Right to object**: if NHS Kernow relies on public or legitimate interests as its legal process for processing an individual's personal data they have a right to object. We must stop processing unless there is a compelling legitimate reason which over-rides the interests, rights and freedoms of the individual.

h) **Rights in relation to automated decision making and profiling**: individuals have right not to be subject to decisions based solely on automated decision making or profiling. When this forms part of an organisation's processes, they must be fair, transparent and able to explain the algorithms that support this decision making, e.g. when applying for a loan.

   NHS Kernow does not tend to rely on automated decision making or profiling.

The Privacy Notice on NHS Kernow's website explains how and when we process personal information and the legal bases we use. We have a responsibility to ensure individuals also know how to invoke their rights and this is typically done through contacting the Data Protection Officer. Should staff receive a request from an individual wishing to discuss or invoke one of their 8 rights, please contact the Data Protection Officer or a member of the Corporate Governance team as a matter of urgency. As noted above, we only have 30 days to action their request or confirm the CCG's reasoning for why this is not appropriate.

10. Subject access request (SAR)

Individuals (such as patients or staff members) have the right to request access to personal information held about them by NHS Kernow, under the Data Protection Act 2018.

If you receive a request, verbally or in writing, for the personal information NHS Kernow holds regarding a living individual, please email this request with as much information as possible to kccg.corporategovernance@nhs.net

The Corporate Governance Team will then ensure this is passed to Cornwall Partnership Foundation Trust who provide the administrative function of the Subject Access Requests on behalf of NHS Kernow.

The Corporate Governance Team will then ask all teams who may have had contact with the individual to provide all records they hold, this includes:

- All clinical records

- Any emails which mention the individual by name or initials
- Any information stored on paper records – such as letters and or handwritten notes
- Any information which may have been archived – this includes recorded conversations and old text messages

NHS Kernow is required to respond to Subject Access Requests within one calendar month. It is therefore imperative that records are provided in a timely manner as the corporate governance team require time to check the records received and redact any third party information.

Failure to respond to the request within the time period can result in fines being levied by the Information Commissioners Office. It is also an offence to knowingly destroy, deface or conceal the information requested. This too can result in fines for NHS Kernow and a possible conviction for a member of staff.

11. Sharing and use of personal information

Where any personal information is used or considered for use by the organisation, there must always be legal basis for that use. Where you share personal information with other organisations for reasons that do not related to direct patient care, certain conditions must be adhered to as set out in the relevant Information Sharing Agreement.

As an organisation we try to work in partnership with other health and social care organisations. However, this does not allow us to share confidential information with them without a lawful basis. Even with a lawful basis, consideration must always be given to the extent of information to be shared and if there are implications for 3rd parties, e.g. family members.

When seeking to share information that does not relate direct patient care, please bear in mind it may be inappropriate to disclose the information unless:

- The individual has given their explicit consent for the information to be used for specific purposes
- There is a legal obligation to disclose the information (e.g. Court Order)
- There is an overriding public interest to disclose the information; you will need to consult with the Data Protection Officer to confirm this.

If in doubt, don't share and ask first!

Please also remember employment and HR records are also considered confidential personal information and the same rigour needs to be applied when accessing these records as it does for patient records.

All staff should be aware that access made to electronic records is recorded and auditable. Audits are run periodically on all systems to check that access made to records is legitimate and required.

As outlined in NHS Kernow's information governance related policies, all staff can be held personally liable for breaches of the Data Protection Act 2018 and may be subject to NHS Kernow's disciplinary procedures, fined and/or and can be prosecuted in addition to NHS Kernow itself being fined by the Information Commissioners Office.

If you have any concerns whatsoever about inappropriate access to, or sharing of, personal data you can speak to your line manager, the Data Protection Officer, SIRO or Caldicott Guardian. They will all be happy to discuss this with you.

12. Information security

Information Security – staff responsibilities

DO…

- Remember that you are bound by NHS Kernow's code of confidentiality
- Be aware of information governance policies and procedures
- Be aware of your responsibilities for information security
- Be aware that unauthorised access to disclosure of or misuse of personal data will be treated as a serious disciplinary offence and will be required to be reported to the Information Commissioner with the possibility of personal fines and/or prosecution
- Ensure that temporary staff and third party contractors complete mandatory Data Security Awareness training
- Remember that you are responsible for ensuring that you are up to date with all mandatory training to enable you to carry out your work efficiently and securely. This is both a contractual and legal requirement and may lead to disciplinary action for you and substantial fines by the Information Commissioner on the Organisation
- Ensure your training needs are assessed on a regular basis
- Report potential concerns or security weaknesses to your line manager
- Know how to report security incidents – the corporate governance team is always available to help
- Be aware that the organisation has a formal disciplinary process for dealing with staff that disregard the organisations' policies and procedures.

DO NOT…

- Attempt to prove a suspected security weakness, as testing a weakness might be interpreted as a potential misuse of the system
- Share passwords or pin codes with other members of staff, not even a manager or CITs
- Allow third parties access to the organisations, hardware and equipment, without correct authorisation
- Be afraid to challenge anyone who you were not aware would be in the organisation
- Ignore security incidents

Physical Security

DO…

- Report the loss of your access keys or identity card immediately to your line manager
- Ensure all IT equipment is reasonably protected against theft and unauthorised access
- Follow the procedures for use of laptops, portable devices, mobile phones and removable media and ensure that if you use a mobile device, that it is password protected
- Ensure that assets are disposed of in accordance with organisational policy, if in doubt ask CITS
- Wear an ID badge
- Ensure visitors have visitor badges so staff can identify those who may not be familiar with organisational policies and restrictions
- Challenge unidentified visitors in controlled areas
- Escort visitors in secure areas at all times
- Ensure confidential and patient information is locked away when not required
- Ensure that confidential waste is disposed of using locked shred-it bins
- Clear confidential and personal confidential information away from printers and fax machines immediately
- Ensure computers are not left logged on and unattended - Ctrl-Alt-Delete then click lock computer or windows key-L
- Ensure keys to filing cabinets and premises are securely stored
- Ensure that secure areas are kept secure and locked when not in use
- Site your computer screen away from unauthorised viewing, if this is not possible request a privacy screen for your device.

DO NOT…

- Take equipment, information or data off-site without prior authorisation
- Leave equipment, information or data unsecured in public areas
- Tell others what keys or access codes you have been entrusted with

13. Caldicott Guardian Log

There is a subtle difference between Information Governance and Caldicott Guardian:

IG = Can you do it legally and how?
Caldicott = should you do it?

The Caldicott report on patient identifiable information in 1997 recommended that “a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient

information." This recommendation was accepted and since 1998 every NHS organisation has been required to have such an individual in post.

A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing

The Caldicott Guardian log is a record of all breaches and near misses of loss of patient information. If you are aware of a breach or of an action that might be classed as a near miss then please report it to the Caldicott Guardian email address kccg.caldicottincidents@nhs.net . This allows the Caldicott Guardian to be aware of any weaknesses in relation to patient information and to advise teams and the organisation appropriately.

If you are thinking of sharing patient information outside of your team and or NHS Kernow then please contact the Caldicott Guardian, the DPO or the Head of Information Governance for advice. This allows for a reasoned discussion and an informed decision to be reached regarding sharing of patient information. The advice given will be logged and can be used should a breach occur or a complaint be made.

The following section outlines how data breaches should be reported and the template for doing so is attached at **Appendix 3**. The seven Caldicott Guardian Principles and the ten Data Security Standards are attached at **Appendix 4**.

14. Reporting information governance data breaches

Internal IG breaches are any incident that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual or organisation, or the loss of personal information. This may include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by an organisation or employee
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission, and,
- loss of availability of personal data

All incidents or information indicating a suspected incident should be reported as soon as possible, and preferably within 24 hours, to the Data Protection Officer (DPO) using the following email address: kccg.caldicottincidents@nhs.net. Please provide as much detail

as possible as this will allow the DPO or Corporate Governance team to determine what action should be taken. The template to use is attached at **Appendix 3 and should be completed and returned within a maximum of 72 hours**.

Externally Reported Breaches

If there is a likelihood the breach may result in a risk to people's rights and freedoms then this will require reporting to the Information Commissioner within 72 hours (not working hours) of the breach occurring. This will be done by the DPO and as part of this we will need your help to report the steps taken to minimise the impact. Therefore, information over and above the reporting template attached at **Appendix 3** may be needed.

Any breaches that are reported to the Information Commissioners Office (ICO) shall be escalated and discussed with the SIRO and/or the Caldicott Guardian. They will also be formally reported to both the Information Governance Sub Committee and Workforce Committee.

As part of the breach reporting process, it is possible we may need to contact the individuals affected by a breach, particularly in those instances when the ICO has been notified. These decisions will be taken on a case by case basis depending upon the circumstances surrounding the breach and the mitigations that have been possible. Should this situation occur, it will be discussed with the staff member and their line manager in order to determine the best way to do this.

Please Do Not…
Keep a breach to yourself. Ensure it is reported not only so that working practices can be improved but because information governance and information security breach reporting is mandated by law and not reporting such breaches could result in substantial fines and prosecution to the organisation and/or yourself.

15. Spot Checks

As part of the assurance process for information governance, the corporate governance team undertake spot checks to ensure computer screens are not left unlocked and that confidential information is not left visible or unsecured.

If the corporate governance team find this is the case they will leave a note for the user to let them know and this will be reported to the appropriate line manager and director. The overview of spot checks will also be reported on a regular basis to the Information Governance Sub Committee and, where appropriate, escalated to the Workforce Committee.

Appendix 1a – Simple DPIA Template

Simple Data Protection Impact Assessment (DPIA)

This form is used when mapping information processes that are deemed to have a low level of risk. The comprehensive DPIA template will need to be completed for areas of medium and high level of risk. If in doubt which template to use please contact the Head of Information Governance or a senior member of the Corporate Governance team for advice.

A DPIA must, as a minimum, contain:

1) a thorough description of the planned processing operations and the **purposes** of the processing, including, where applicable, the legitimate reasons **for processing the data**
2) an assessment of the **necessity and proportionality** of the processing operations in relation to the **purposes**
3) an assessment of the **risks to the** rights **and freedoms of data subjects**
4) the measures intended to **address** the risks, including **safeguards, security** measures and mechanisms to ensure the protection of personal data and to **demonstrate compliance** with the General Data Protection Regulations (GDPR) with regard to the rights **of data subjects** and other persons concerned

Area/Function DPIA Covers:	
DPIA completed by:	
Job Title:	
Department:	
Date:	

STEP 1 – Identify why a DPIA is needed:
Explain broadly what the project/functional area/procedure aims to achieve and what type of processing of personal data it involves. i.e. *Why do you have and use personal data?*

STEP 2 – Describe the data processing expected
(i) What processing is needed: • What is the source of the data you will collect, use or store? • What are you doing with the data? • Who will you share it with? • When will it be deleted?
(ii) What's within its scope: • *What will the data include and for how many individuals?* • *How much will be collect and how often?*
(iii) What's the context of the processing: • *What is the nature of your relationship with the individuals?* • *How do they know what their information is being used and how much control will they have?* • *Are there any known current issues of public concern?* • *Do we have a known legal basis for processing the data, e.g. relates to direct patient care, explicit consent, inferred consent, do individuals expect us to use their data information in this way, etc.*
Suggested legal basis for processing (see "Key Notes" on final page for more information)**:**
(iv) Describe the purposes of the processing: • *What do you want to achieve?* • *What is the intended effect on individuals?* • *What are the benefits of the processing for the organisation?*
STEP 3 – Discussions already held/consultation process/internal processes in place • *Who have you spoken to?*

• *What advice have you received?* • *What outstanding queries need answering?*
STEP 4 – Assess necessity and proportionality • *How are you minimizing the amount of personal data processed?*
STEP 5 – Identify and assess risks - Outline the risks considered taking account of the following areas (which is not considered to be an exhaustive list): • *Where and how will the data be received and stored?* • *Is the information backed up?* • *Who has access and is the level of access controlled at an individual level?* • *How is the information distributed?* • *Is a contract or Data Sharing Agreement (DSA) needed and if so, is it in place?* • *Is a business continuity plan (BCP) needed and if so, is it in place?* • *Is information transferred outside of the UK?* • *Is there an agreed data disposal/retention period? How is data disposed of appropriately?*
STEP 6 – Identify measures to reduce risk – what mitigations are planned or already in place? What additional support do you need based on Step 5 above?
STEP 7a – Sign off and record outcomes – by Head of Department (not the individual completing the form above)

Measures, risks and mitigations approved by: [Name and job title]	
Date:	
Comments:	

STEP 7b – Head of IG/DPO Advice – to advise on/ensure compliance and review dates	
Head of IG/DPO advice provided by:	
Date:	
Summary of Head of IG/DPO advice: Additional columns in database to be added to identify retention period and date for disposal which will then need recording in the Disposal Schedule.	
Confirm lawful basis for processing: *(* Delete where not applicable)*	Consent / contract / legal obligation / vital interests / public task / legitimate interests *
This DPIA will be kept under review by: **[Name and job title]**	
Expected date of review:	

Please return completed form to: kccg.corporategovernance@nhs.net

STEP 8 - For Corporate Governance Team Use Only	
DPIA reference no:	
Title used:	
Date logged:	
Legal basis for processing:	
Planned review date:	

Key Notes:

Lawful processing of information must be in accordance with one of the reasons given below. Article 6(1) of the General Data Protection Regulations refers.

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 1b – Comprehensive DPIA Template

The Comprehensive DPIA template may need to be used in exceptional circumstances where there is a high risk of breaching the data protection rights and freedoms of individuals. This too can be found on the Document Library.

The corporate governance team is able to advise which is the most appropriate template to use.

Comprehensive Data Protection Impact Assessment (DPIA)

A DPIA must, as a minimum, contain:

1) a thorough description of the planned processing operations and the **purposes** of the processing, including, where applicable, the legitimate reasons **for processing the data**
2) an assessment of the **necessity and proportionality** of the processing operations in relation to the **purposes**
3) an assessment of the **risks to the** rights **and freedoms of data subjects**
4) the measures intended to **address** the risks, including **safeguards, security** measures and mechanisms to ensure the protection of personal data and to **demonstrate compliance** with the General Data Protection Regulations (GDPR) with regard to the rights **of data subjects** and other persons concerned

Area/Function DPIA Covers:	
DPIA completed by:	
Job Title:	
Department:	
Date:	

STEP 1 – Identify why a DPIA is needed Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

STEP 2 – Describe the data processing
(v) Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
(vi) Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
(vii) Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? Do we have a known legal basis for processing the data?
Suggested legal basis for processing (see "Key Notes" on final page)**: xxx**
(viii) Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for the organisation?

STEP 3 – Consultation process **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

STEP 4 – Assess necessity and proportionality **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

STEP 5 – Identify and assess risks – as a minimum, please ensure the following areas are covered. The list is not exhaustive.

- Where and how will the data be received and stored?
- Is the information backed up?
- Who has access and is the level of access controlled at an individual level?
- How is the information distributed?
- Is a contract or Data Sharing Agreement (DSA) needed and if so, is it in place?
- Is a business continuity plan (BCP) needed and if so, is it in place?
- Is information transferred outside of the UK?
- Is there an agreed data disposal/retention period? How is data disposed of appropriately?

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. *(Please add more rows, if needed)*	**Likelihood of Harm** (Remote, possible or probable)	**Severity of Harm** (Minimal, significant or severe)	**Overall Risk** (Low, medium or high)

1)			
2)			
3)			
4)			
5)			

STEP 6 – Identify measures to reduce risk			
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5. *(Please add more rows, if needed)*	**Effect on risk** (Eliminated, reduced or accepted)	**Residual risk** (Low, medium or high)	**Measure approved** (Yes/No)
1)			
2)			
3)			
4)			
5)			

STEP 7a – Sign off and record outcomes – by Head of Department (not the individual completing the form above)	
Measures approved by: **[Name and job title]**	
Date:	
Comments: *(Please ensure actions are integrated back into project plan, with date and responsibility for completion.)*	
Residual risks approved by: **[Name and job title]**	

Date:	
Comments: *(If accepting any residual high risk, DPO to consult the ICO before going ahead)*	
STEP 7b – Head of IG/DPO Advice – to advise on/ensure compliance and review dates	
Head of IG/DPO advice provided by:	
Date:	
Summary of Head of IG/DPO advice: *(DPO will advise on compliance, Step 6 measures and whether processing can proceed)*	
DPO advice accepted or overruled by: [Name and job title]	
Comments/for what reason:	
Consultation responses reviewed by: **[Name and job title]**	
Comments: *(If the decision departs from individuals' views, explain reasoning)*	
This DPIA will be kept under review by:	

[Name and job title]	
Expected date of review:	

Please return completed form to: kccg.corporategovernance@nhs.net

STEP 8 - For Corporate Governance Team Use Only	
DPIA reference no:	
Title used:	
Date logged:	
Planned review date:	

Key Notes:

Lawful processing of information must be in accordance with one of the reasons given below. Article 6(1) of the General Data Protection Regulations refers.

g) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

h) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

i) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

j) **Vital interests:** the processing is necessary to protect someone's life.

k) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

l) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 1c – DPIA frequently asked questions

What is a Data Protection Impact Assessment?
A Data Protection Impact Assessment (DPIA) is an assessment of the personal data that is held and used by the organisation. It assesses how and why we have personal information and how long we will keep it.

Why do we need to do this?

The new GDPR says that an impact assessment should be carried out for any personal data the organisation uses or processes. It should help the organisation be compliant with GDPR, by highlighting why the organisation has the personal information and what they are doing with it and why.

When do we need to do one of these?

Your team must complete one of these for all information it currently holds. Then one should be completed prior to processing/using personal data in a new or different way. If you create a new spreadsheet, database, any record that uses personal data in a new way then you need to complete a DPIA.

What is classed as personal data?

Any information that is clearly about a particular person such as, but not limited to:

- Name
- Date of birth,
- Address
- Email
- NHS Number
- NI Number
- Photograph
- CHC number
- IP address
- Clinical history
- Any other local identifier

The qualifier ‘certain circumstances’ is worth highlighting, because whether information is considered personal data often comes down to the context in which data is collected. Organisations usually collect many different types of information on people, and even if one piece of data doesn’t individuate someone, it could become relevant alongside other data.

For example, an organisation that collects information on people who download products from their website might ask them to state their occupation. This doesn’t fall under the GDPR’s scope of personal data, as, in all likelihood, many people have that occupation. Similarly, an organisation might ask what company they work for, which, again, couldn’t be used to identify someone (unless they were the only employee). However, when collected together, these pieces of information could be used to narrow down the number of people

to such an extent that in many instances you could reasonably establish someone's identity.

What are the legal reasons for having personal data?

The GDPR states there are only 6 reasons for having and using/processing data

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests**: the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you cannot respond yes to one of the above then the information should not be held. Please contact the Corporate Governance Team to discuss further.

What are retention schedules?

Retention schedules set out the length of time personal and organisational records should be kept. NHS organisations use the Records Management Code of Practice for Health and Social Care 2016 to determine. However, not all records are covered in this, and if you cannot find a record you have in this schedule please contact the corporate governance team who will be able to support you in determining the length of time the records should be retained.

When and how should we dispose of information?

Once information has reached the end of its retention period then we are required to review if it is information we should be keeping. For example we are required to keep complaints records for 10 years in case of legal challenge, however at the end of the 10 year period it would be wrong to throw it all away just because it is 10 years old as there may be cases which we require to be kept because of litigation, or further challenge. However, one would expect the majority of the cases to be no longer required.

All paper copies of information should be placed in confidential shredding and all electronic files should be deleted permanently. A record of destroyed information should be retained on a Disposal Schedule.

What is a disposal schedule?

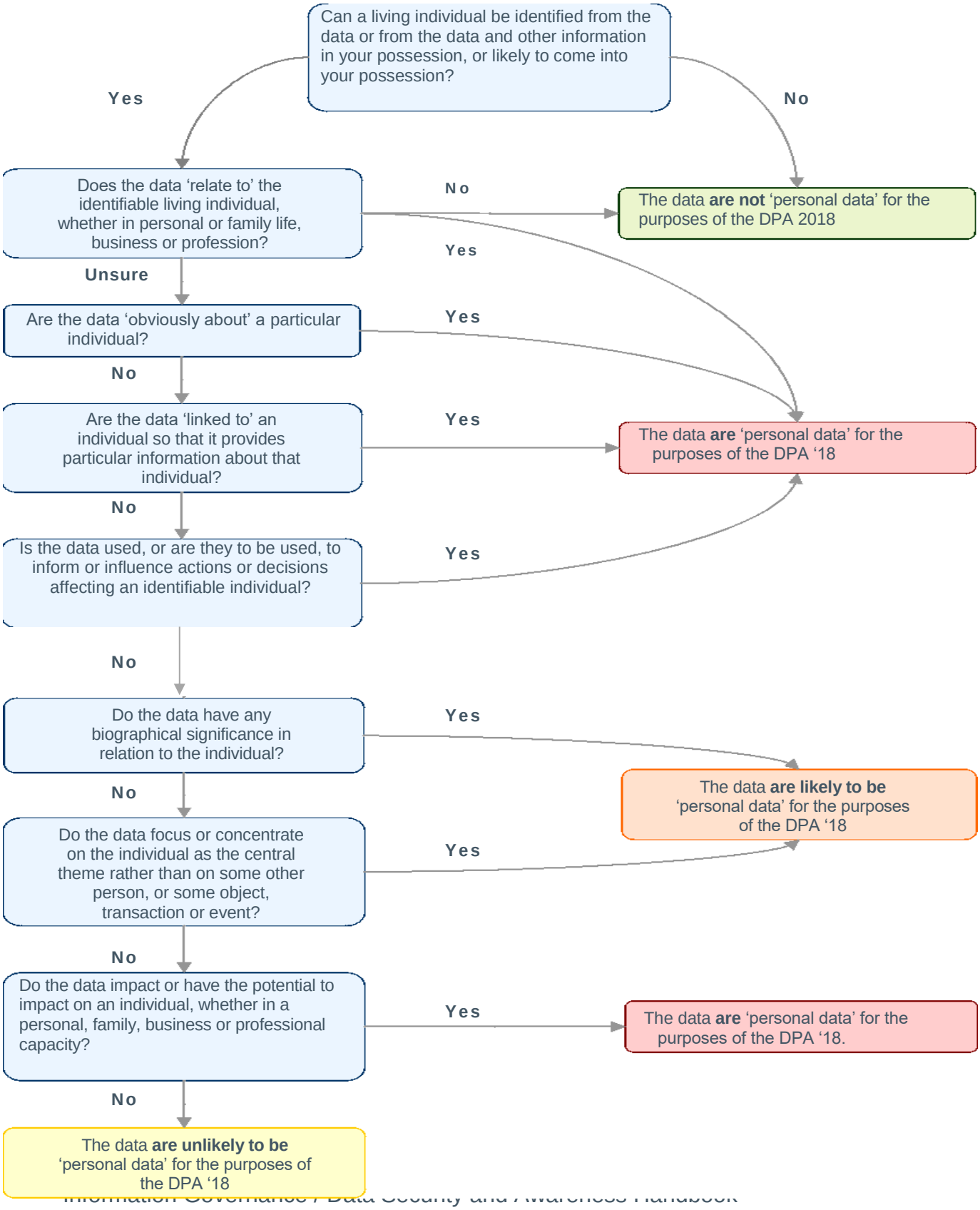
A disposal schedule is a record of files deleted and or destroyed when they have reached the end of their retention period. It is important to keep a record of what is disposed of, when it was disposed of and why. For example, you may keep a disposal schedule that states on 01/01/2018 you deleted all personal information relating to the engagement process for patient transport as this was at the end of the retention period and no longer required, nor part of a complaint.

A disposal schedule is important for all organisational and personal information.

Why do we need a disposal schedule?

The Information Commissioner identifies that a disposal schedule contributes to the good management of records, particularly those held by public authorities. They will allow the authority to know the location of information it holds or that which has been transferred to archives, or whether the information has been destroyed and, if so, why and when. If information personal or organisational is later requested a disposal schedule allows an organisation to prove information was held and why and when it was destroyed.

Appendix 2 Personal data flow chart



NHS
Kernow
Clinical Commissioning Group

Appendix 3 - Information Governance Incident Report Template

Please see the Data Protection Policy and Incident Management Policy or speak to the Corporate Governance team for support with completing this form.

Once completed, please return form to: kccg.caldicottincidents@nhs.net

Date of incident:	
Time of incident:	
Description of what happened:	
Actions taken:	
Lessons learned:	
Completed by: **[Name and Job Title]**	
Signed:	
Date:	

For use by Corporate Governance Team: Log No: xxx	**Date advised of incident:** **Date incident form received:** **Date logged on database:**	

Appendix 4 – Caldicott guardian principles and data security standards

a) The seven **Caldicott Guardian Principles** are:

Principle 1 - Justify the purpose(s) for using confidential information

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

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

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

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

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

Principle 6 - Comply with the law

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

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share Or Not To Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

b) The ten **National Data Guardian's (NDG) Data Security Standards** are outlined below. They are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation. As can be seen the standards are divided amongst three leadership obligations.

Leadership Obligation 1: People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate. Data Security Standard Overall Guide

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Appendix 5 – Other inclusions

If there is anything further you would like to see added to the handbook please contact the corporate governance team by emailing kccg.corporategovernance@nhs.net