

# INFORMATION GOVERNANCE

Staff Handbook 2020-21



**NHS**

**Brighton and Sussex  
University Hospitals**  
NHS Trust

**NHS**

**Western Sussex Hospitals**  
NHS Foundation Trust



**For use by all Staff, including  
employees, bank, locum, agency workers,  
contractors, office holders and volunteers,  
as required by the Trusts'  
Information Governance Policies**

**Current version: v6.0, September 2020  
Next review: September 2021**

## **STAFF CONFIDENTIALITY CODE OF CONDUCT**

### **For all staff, including Employees, Bank, Locum, Agency Workers, Contractors, Office Holders and Volunteers**

This Code outlines your responsibilities in protecting the personal data you come into contact with during your employment with the Trust. It has been produced to ensure you are aware of your legal duty to maintain confidentiality and is issued with every employment contract.

Personal data means any information (paper, electronic, tape, verbal, etc.) from which an individual can be identified either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. It also relates to sensitive personal information including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic / biometric data, health, data concerning sex life or sexual orientation. This Code applies to the data of both living and deceased individuals.

### **Know Your Obligations**

All staff have a duty of confidentiality regarding personal information. This is based on Data Protection and other laws, decisions made about the law in Courts, employment contracts and, for registered health and some other practitioners, under professional obligations and codes of conduct. Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution as well as opening the Trust to legal claims and the potential of significant fines.

Therefore you must not:

- Put personal information at risk of unauthorised access.
- Misuse any personal information or allow others to do so.
- Access information, including your own, without a legitimate reason to do so as part of your job.

## **Keep Personal Information Private**

You must comply with the rules laid out in the Trust's **Information Governance Policy** and the **Information Governance Staff Handbook**, both of which are available in full on the **Intranet**. The **Handbook** in particular sets out practical steps to take to keep personal data protected.

## **Disclose with Appropriate Care**

The Trust will ensure that patients and staff are adequately informed about the use and disclosure of their personal information by the use of Privacy Notices and leaflets which will tell them how and why their personal information is used. You must ensure you are familiar with this patient information material and seek advice from the Information Governance Team if you are asked questions you are unable to answer.

If you are authorised to disclose personal information you must only:

- Share with those with a legitimate right to see / hear the information.
- Transfer information in line with the Trust's secure transfer methods.
- Disclose the minimum necessary to provide safe care.

Under Common Law, identifiable information may be disclosed without consent when:

- There is a legal duty to do so, for example a Court Order;
- It is necessary to safeguard the individual, or others, or is in the public interest, such as where the public good outweighs obligation of confidentiality to the individual concerned.

During office hours, refer all requests for disclosure of personal information without the consent of the individual, including requests from the police, to the Information Governance Team. Out of hours these must be referred to the Site Manager. All decisions to disclose must be fully documented.

## **IMPORTANT NOTICE**

**This document comprises advice based on Frequently Asked Questions, concerns and issues about which the Information Governance Team are aware. It is published as generic guidance only. The Information Governance Team does not and cannot accept responsibility for detailed or complex Information Governance decisions that are taken without its bespoke input.**

**All information and URL links in this document are believed to be correct at time of publication.**

**If you have any comments or suggestions regarding the content of this *Handbook*, please contact the Information Governance Team using the details in the Appendix.**

**Any suitable comments or amendments will be incorporated at the next review, due to be published in autumn 2021.**



## Contents

	Staff Confidentiality Code of Conduct	2
	Preface	6
	Acronyms	7
	Introduction	8
Chapter 1	The Trust's Information Governance Staff	9
Chapter 2	Legislation, Regulations, Guidance and Trust Policies	11
Chapter 3	Caldicott Principles, Data Protection Law and Consent	12
Chapter 4	Guide to Confidentiality	13
Chapter 5	Social Media and the Use of Mobile Phone-based Messaging Apps	19
Chapter 6	Parental Responsibility	20
Chapter 7	<b>NEW!</b> Use of Childrens' Information	23
Chapter 8	Subject Access Requests	23
Chapter 9	Management of Clinician to Clinician Handover Sheets	24
Chapter 10	Sharing Information with the Police	25
Chapter 11	Information Governance and Cyber Security Breaches	26
Chapter 12	Decommissioning Work Areas: Checking for Confidential Information	27
Chapter 13	Monitoring Access to Personal Confidential Data	28
Chapter 14	Information and Cyber Security	28
Chapter 15	Use of Email	31
Chapter 16	Photography and Recordings	33
Chapter 17	Video Consultations	36
Chapter 18	Information Governance Mandatory Training	37
Chapter 19	Records Management	38
Chapter 20	<b>NEW!</b> Working from Home	40
Chapter 21	Storage of Locally-Held Staff HR Records	41
Chapter 22	Freedom of Information Requests	42
Chapter 23	Data Protection Impact Assessments	43
Chapter 24	Business Continuity	44
Chapter 25	Information Sharing	44
Chapter 26	<b>NEW!</b> Next of Kin	45
Chapter 27	Research	46
Chapter 28	Use of Information for Non-Care Purposes	47
Chapter 29	The National Data Opt-Out	48
Chapter 30	Smartcards	49
Chapter 31	Data Quality	50
Chapter 32	When Staff Become Patients	50
Chapter 33	Management of Third Party Contracts	51
Chapter 34	Counter Fraud	53
	Appendix 1: Contact Details	55
	Appendix 2: Staff Employment Records Privacy Notice	57
	Consultation, Distribution and Acknowledgements	61

## Preface

Dear colleagues

We are delighted to welcome you all to this significantly updated Sixth Edition of the *Information Governance Staff Handbook*, the third time it has been published as a joint venture between Brighton & Sussex University Hospitals NHS Trust and Western Sussex Hospitals NHS Foundation Trust. It complements the annual mandatory Information Governance (IG) Training programme which all staff are required to undertake and has been designed as first resource for your IG queries, covering many of the FAQs that the IG Team is regularly asked.

To ensure the *Handbook* is as up-to-date, relevant and accessible to you as possible, the IG Team have:

- Updated it with comments and suggestions received since the publication of the Fifth Edition.
- Liaised widely across both Trusts to ensure it covers your needs.
- Agreed a distribution plan with the IG Steering Group so everyone either gets a copy, or knows from where it is available.

It is well over two years since the **EU General Data Protection Regulation 2016** and **Data Protection Act 2018** became applicable in the UK, and the IG Team has been working hard to apply it to our real world, working in a fast-paced healthcare environment, never more so than in the unprecedented times 2020 has brought with it. Real-life examples, as well as the news stories we mentioned above have shaped that understanding and helped form the interpretation in this *Handbook*.

Even with a two years having passed, the IG Team is also still learning, and working hard to offer advice, but do be patient with them, as they still have very little case law to work from, which means advice and guidance may change and mature over time.

On that note, if you need specific IG advice and support, please do not hesitate to contact the team using the details in the Appendix of this *Handbook*. Or, if you have a specific query relevant to our roles, equally, please do not hesitate to contact us (summaries of our roles are in Chapter 1).

██████████  
Group Director of IM&T  
**Senior Information Risk Owner**  
BSUH and WSHFT

██████████  
Consultant Paediatrician  
**Caldicott Guardian**  
WHSFT

██████████  
Medical Director  
**Caldicott Guardian**  
BSUH

██████████  
Group Head of Information Governance  
**Data Protection Officer**  
BSUH and WSHFT

*3 September 2020*

## Acronyms

BCP	Business Continuity Plan
BSUH	Brighton and Sussex University Hospitals NHS Trust
CCG	Clinical Commissioning Group
DH	Department of Health and Social Care
DPA18	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation 2016
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
PAS	Patient Administration System (i.e. Medway at BSUH, SemaHelix at WSHFT)
PBAC	Person-Based Access Controls
PCD	Personal Confidential Data (see p.9 for full definition)
RA	Registration Authority
SAR	Subject Access Request
SIRO	Senior Information Risk Owner
WSHFT	Western Sussex Hospitals NHS Foundation Trust

## Introduction

Information Governance (IG) is the practice used by all NHS organisations to ensure that information is efficiently and legally managed. To achieve this, appropriate policies, processes and management accountabilities have been put in place to ensure a robust framework for the safeguarding of information.

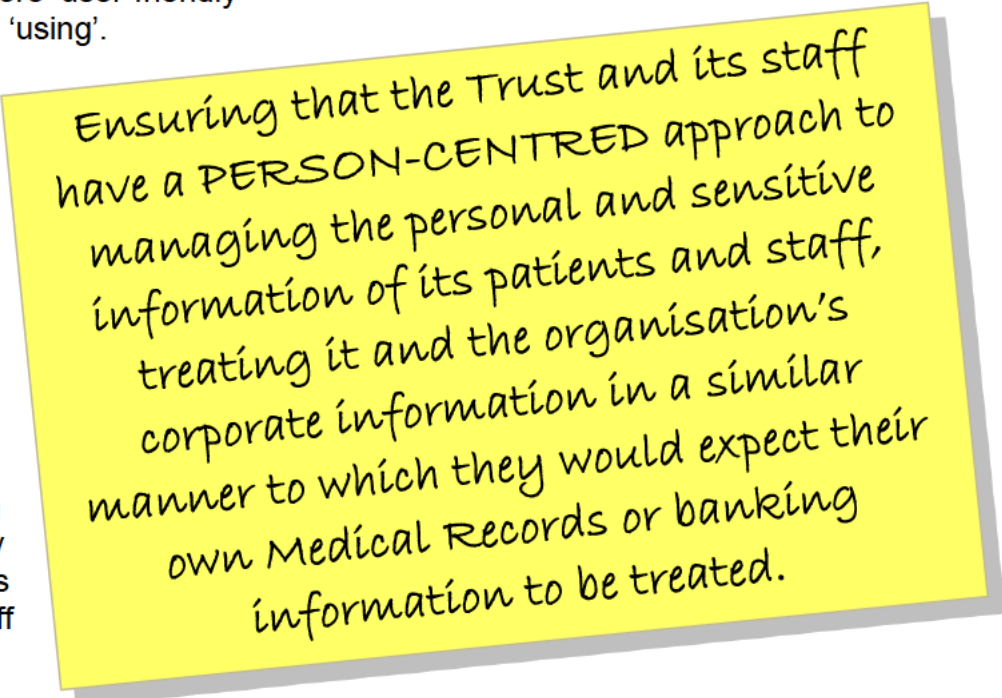
In turn, the *Information Governance Staff Handbook* has been produced to support you by giving information and sign-posting you to guidance so you are effectively informed in your work and decision-making when using personal and sensitive information. It has been written taking full account of the IG requirements from the Department of Health and Social Care (DH) Data Security and Protection Toolkit (**DSPT**) (see p.11), which sets out robust guidelines with regard to IG. FAQs received by the IG Team have been taken into account in this edition of the *Handbook*, and it is reviewed annually.

Throughout this document, the term **Personal Confidential Data (PCD)** is used; it is defined on the blackboard on p.9.

Anything we do with PCD, from the point it is created to the point it is appropriately disposed of, is defined as processing. A more user-friendly word than processing may be 'using'.

The definition of IG the Trust works to is simply stated, as on the yellow Post-It note.

NHS organisations hold vast amounts of PCD, and all staff should be able to provide assurance that the IG standards are incorporated within their working practices. PCD can be contained within a variety of documents, such as Medical Records and staff files.



Ensuring that the Trust and its staff have a **PERSON-CENTRED** approach to managing the personal and sensitive information of its patients and staff, treating it and the organisation's corporate information in a similar manner to which they would expect their own Medical Records or banking information to be treated.

Other sensitive information may be held in corporate documents such as contracts, minutes and finance documentation.

All staff are required to keep all patient and staff information confidential unless disclosure is expressly authorised by the Trust.

**Knowingly misusing of or a failing to properly safeguard any confidential data will be regarded as a disciplinary offence.**



*The term PERSONAL CONFIDENTIAL DATA applies to all identifiable individuals, including patients and staff, including those who have passed away, for whom there is a responsibility to maintain confidentiality. The type of information includes:*

- Personal Data: e.g. name, unique identification numbers (such as NHS, hospital or National Insurance number), location data, online identifiers or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person.*
- Special Categories of Sensitive Data: e.g. ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data (both physical and mental), sex life, sexual orientation or data relating to criminal activity.*

## Chapter 1: The Trust's Information Governance Staff

Within the Trust there is a multi-layered IG structure:

### a. Accountable Officer

The individual with overall accountability for IG within the Trust is the Accountable Officer. This is the Chief Executive. The role is to provide assurance, through a "Statement of Internal Controls", that all risks to the organisation, including those relating to information, are effectively managed and mitigated. The Chief Executive is [REDACTED]

## b. Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) must be a Director-level member of staff or member of the Senior Management Board. They have overall responsibility for the organisation's information risk policy. The SIRO also leads and implements the IG risk assessment and advises the Board on the effectiveness of information risk management across the organisation. The SIRO is supported by the IG Team. The role is held by [REDACTED], Director of IM&T.

## c. Caldicott Guardian

The Caldicott Guardian is the person within the Trust with advisory responsibility for protecting patient confidentiality and ensuring it is shared appropriately and securely; often they are defined as "the conscience of the organisation". The role is held at BSUH by [REDACTED], Medical Director (left), and at WSHFT by [REDACTED], Consultant Paediatrician (right).

## d. Data Protection Officer

The Data Protection Officer (DPO) role is a statutory requirement under the **EU General Data Protection Regulation 2016** (GDPR) for public authorities such as NHS Trusts. DPOs are responsible for overseeing the organisation's Data Protection strategy and its implementation to ensure compliance with **GDPR** requirements. The role is held by [REDACTED] Group Head of Information Governance.

## e. IG Team

The IG Team is responsible for ensuring that the IG programme is implemented throughout the Trust, including the completion and annual submission of the Trust's DSPT (see p.11). It also supports the Trust in coordinating IG Notifiable Incidents, offering advice and ensuring the organisation complies with legislation, policies and protocols, including training all staff.

The members of the team are:

- [REDACTED] Information Governance Manager (primarily BSUH)
- [REDACTED] Operational Information Governance Lead (primarily BSUH)
- [REDACTED], Group Head of Information Governance / DPO (BSUH and WSHFT)
- [REDACTED], Information Governance Manager (primarily WSHFT)
- [REDACTED] Information Governance Manager (primarily WSHFT)
- [REDACTED] Information Governance Manager (primarily BSUH)
- [REDACTED] Information Governance Manager (primarily BSUH)

Both Trusts also have dedicated IG staff that process patient Subject Access Requests (SAR) (See Chapter 8).

## f. Information Asset Owners

The SIRO is supported across both Trusts by Information Asset Owners (IAO). Their role is to understand what information is held, how it is managed and who has access and why to information systems in their own area. As a result they are able to understand and address risks to the information assets they own and to provide assurance to the SIRO on the security and use of those assets. The IG Team support the IAOs in fulfilling their role. Should you need to contact an IAO for a specific system, the IG Team will be able to assist you as to who they are.

## Chapter 2: Legislation, Regulations, Guidance and Trust Policies

### a. Legislation, Regulations and Guidance

Staff should be aware of the legislation and guidance surrounding IG that direct how healthcare organisations must safeguard information, what processes are in place to use, secure and transfer information. Also how patients and members of public have access to personal / business information. The organisation must comply with, among others:

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- *Confidentiality: Good Practice in Handling Patient Information* (GMC: 2017)
- Data Protection Act 2018
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- General Data Protection Regulation 2016
- Health and Social Care Act 2012
- Health and Social Care (National Data Guardian) Act 2018
- Health and Social Care (Safety and Quality) Act 2015
- Health Service (Control of Patient Information) Regulations 2002
- Human Rights Act 1998
- *Records Management Code of Practice for Health and Social Care* (2016)
- *Information: To Share or Not to Share* (2013) [Caldicott2]
- *Manual for Caldicott Guardians* (2017)
- Privacy and Electronic Communications Regulations 2003
- *Report on the Review of Patient-Identifiable Information* (1997) [The Caldicott Report]
- *Review of Data Security, Consent and Opt-Outs* (2016) [Caldicott3]
- *Safe Data, Safe Care* (2016)



### b. Data Security and Protection Toolkit

From all of this legislation, advice and guidance, NHS Digital manages the **DSPT**. This is a term that will be used throughout the *Handbook*; it:

- Is an online self-assessment tool mandated for use by NHS, social care, GPs, commercial third parties and other providers of NHS/healthcare-related services to self-assess their IG compliance.
- Has 40 requirements, known as Assertions.
- Creates a year-long IG compliance work programme each financial year, facilitated by the IG Team.
- Is subject to both informal internal peer review and formal internal audit.
- Has reports available online showing the level at which each organisation has scored.
- Supports the Trust in bidding for services being commissioned by Clinical Commissioning Groups (CCG) by demonstrating good IG practice within the organisation.

### c. Trust Policies

To support the completion of the work programme, there are a suite of policies, processes and procedures, based on this legislation and guidance. These are listed by name in the respective Trust's **Information Governance Policy** on the **Intranet**.



Adherence to IG principles ensures compliance with the law, best practice and embeds processes that help staff manage PCD appropriately. It must also be noted that embedding IG processes enables patients and service users to have greater confidence in the Trust and enables effective working across partner organisations.

Patients are made aware of the information held about them and what is done with it by posters in public areas directing them to a Privacy Notice leaflet that is held in Receptions, waiting areas, Patient Advice and Liaison Service (PALS) offices and the Trust website.

## Chapter 3: Caldicott Principles, Data Protection Law and Consent

### a. The Caldicott Principles

There are seven Caldicott Principles to be considered when using patient PCD:

1. Justify the purpose(s)
2. Don't use PCD unless it is absolutely necessary
3. Use the minimum necessary PCD
4. Access to PCD should be on a strict need to know basis
5. Everyone with access to PCD should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

The Principles are currently undergoing a National Review, led by the National Data Guardian, Dame Fiona Caldicott. It is expected that a new Principle will be added, to cover the “reasonable expectations” of patients regarding the use of their data. Future editions of this *Handbook* will include any changes that come out of that review.

### b. Data Protection Legislation

All organisations in the UK must comply with the **GDPR** and the **Data Protection Act 2018 (DPA18)**, both of which are enforced in the UK by the Information Commissioner's Officer (ICO), which has the power to fine organisations up to the equivalent of €20m or 4% of turnover (whichever is higher) for Data Protection breaches. Some examples of breaches are given in Chapter 10.



It is unlawful to obtain or disclose personal data or unlawfully sell / offer to sell it on, as happened in 2013 when a pharmacist from another Trust was found to be accessing Medical Records of family members, work colleagues and local health professionals. He was personally fined. **Staff could face disciplinary proceedings which may result in dismissal or being struck off a professional register.**

There are seven **GDPR** principles that must be followed when handling PCD:

1. Use it lawfully, fairly and transparently
2. Use it only for the purpose it was collected
3. Use the minimum amount of data necessary for the purpose
4. Ensure it is accurate
5. Do not keep it longer than needed.
6. Keep it secure
7. Retain records of decisions made to demonstrate accountability

Data Subjects also have increased rights under the **GDPR**, compared to the previous legislation. These are:

1. To be informed how their data is used
2. To access copies of their data
3. To rectification of data when it is incorrect
4. To be forgotten (*although this is rarely possible in healthcare*)
5. To restrict processing unless the Data Subject allows it
6. To move electronic information to another organisation
7. To object to processing of their data
8. To appropriate electronic decision-making

With the exception of the right of access, most requests regarding application of these rights will initially be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law over time.

Full guidance regarding the **GDPR** is available on the [ICO's website](#) and **DPA18** is available on the government's [Legislation website](#).

### c. Consent to Use Information for Direct Care

Sharing and use of information about individuals within and between partner agencies is vital to ensure co-ordinated and seamless provision of Direct Care to patients. Generally consent is not required under the **GDPR** as there is a specific clause within in the legislation that allows, even promotes, sharing for Direct Care.

However, practitioners must maintain an awareness of the **Common Law Duty of Confidentiality**, that if the patient disclosed information in circumstances where it was expected that a duty of confidence applied, it should not normally be further disclosed without that Data Subject's consent. If this has not been obtained it is the responsibility of the member of staff intending to share personal information to make and document an appropriate decision based on whether disclosure is essential to safeguard either patient or a third party, is considered to be in the public interest, or if there is a legal obligation to share the information, such as a Court Order.

Further advice is obtainable from the IG Team.

## Chapter 4: Guide to Confidentiality



Confidentiality in the NHS has been guided for 17 years by the [Confidentiality NHS Code of Practice](#) (2003). Despite its age, this is still a current document that sets out required standards of practice concerning confidentiality.

To compliment the national Code, the Trusts have a **Confidentiality Code of Conduct**, which is issued to at recruitment, reproduced in the front of this *Handbook* and available for everyone on the **Intranet**.

Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential manner. Staff who have access to information about individuals (whether patients, staff or others) must use it effectively, whilst maintaining appropriate levels of confidentiality. This section sets out the key principles and main 'Do's and Don'ts' that everyone should follow to achieve this for both electronic and paper records.

PCD may be manually-held or automated and includes for example, the contents of filing cabinets, all patient information, including Medical Records, photographs, x-rays, and other images, tapes,



CD ROMs, removable media and / or any other emergent technology. Personnel records are also included, and include those held by line managers, as well as, those held centrally by HR. Use of PCD about patients is guided by the Caldicott principles. The **Access to Health Records Act 1990** was largely superseded by Data Protection legislation, but still applies to records of the deceased.

These principles translate into key rules for all staff to follow:

- Patients and staff must be fully informed about how their information may be used.
- There are strict conditions under which personal data may be disclosed.
- Certain disclosures are not allowed without the explicit unambiguous consent of the individual.
- Individuals can see and have copies of information held about them, and have errors corrected.
- PCD should be anonymised wherever and whenever possible.
- The legitimate use or disclosure of PCD is not a confidentiality breach.
- Sharing of PCD between organisations can take place with appropriate safeguards.
- Sometimes a judgement has to be made about the balance between the Duty of Confidence and disclosure in the public interest; any such disclosure must be justified and recorded.
- PCD must be kept secure and confidential at all times.

**It is important to note, if you are considering sending PCD to CCGs there needs to be full and careful consideration as to the legality, as CCGs are not generally permitted to have it. Any such decision taken to share PCD must be documented and agreed in discussion with the IG Team, the SIRO and / or Caldicott Guardian. This should then be stored within the sharing department.**

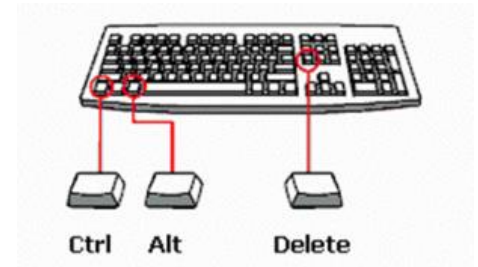
Staff should check with the IG Team if they have any queries on whether to access or process PCD.

**Following some basic principles helps keep information secure and confidential:**

#### **a. Limiting Unnecessary Access to Personal Information**

- Do not discuss confidential matters outside of work, during breaks in public areas, or with anyone at work who does not need to know it; be aware that other people may overhear, particularly in wards, corridors and open plan offices.
- Do not disclose who you see in any of the hospitals to anyone else, even if they are only met casually in public areas. To do so may breach a confidence of which you are unaware.
- Do not leave working papers lying around the ward or office, including in in-trays.
- Remove documents from photocopiers immediately.
- Hold keys and other access means, such as ID cards and combinations of locks, securely away from the point of use. Ensure that there is an appropriately secure system in place to allow access in event of emergency or an individual's absence.
- Keep offices locked when unoccupied, and maintain overall building security. Be aware of people, whether staff, patients or general public, who may not have access to certain areas but try and 'tailgate' you into a secure environment.
- Keep workstations and other computer equipment secure, being particularly careful with laptops when not in use, especially not leaving them unattended in vehicles or public places.
- Lock away portable equipment containing PCD or other confidential information when not in use.
- Ensure cabinets containing PCD are locked when unattended.
- Passwords must be a combination of letters and digits, and combination of characters, a mixture of upper case and lower case letters. In systems you may use special characters, such as ? and !

- Passwords must not be written down, unless this is encrypted.
- Ensure that computer monitors cannot be seen by people, especially in public Receptions.
- Lock your computer when you are not using it, even for short periods, by using 'Ctrl-Alt-Del' (located as demonstrated in the picture, right), and selecting Lock from the options.
- Do not allow **anyone** else, including your line manager or IT, to use your log-on to any Trust computer or computer system. To do so breaches the **Computer Misuse Act 1990**.



#### **b. Ensuring Authorised Access Only**

- Access to records is based on the appropriateness of access by role, in line with Caldicott Principle 4 that access to PCD is on a strict need to know basis. For electronic systems it is governed by a process called Person-Based Access Controls (PBAC).
- If you are an IAO, ensure all staff role changes are accurately reflected in PBAC. Staff moving between departments may require either more or less access levels to systems.
- All holders of swipe cards must be aware that the Trust may monitor and investigate swipe card records for the following reasons, to:
  - Ensure compliance with Trust policies.
  - Govern access management privileges.
  - Collate data for authorised outside agencies, e.g. the police, for counter fraud investigations.
  - Audit for authorised HR investigations.
- There is no automatic right of access to records and access must be agreed in advance with the respective IAO. Ideally this is with auditable written permission.
- Do not store PCD on the hard drive of any laptop or PC: always use network folders that have access controls.
- Never send PCD outside the Trust without appropriate level of authorisation or protection.

#### **c. Accuracy, Retention and Disposal**

- If adding information to records, satisfy yourself of its current accuracy and relevance.
- If you are an IAO ensure that records are held with an appropriate legal basis, are relevant for the purpose held, and are kept accurate and up-to-date. Records must be retained in line with the [Records Management Code of Practice for Health and Social Care](#) (2016).
- Ensure any unneeded PCD on paper is confidentially destroyed. Do not use it as scrap paper. Ordinary bins and 'recycling' bins must not be used for papers containing PCD.
- Dispose of redundant equipment containing PCD by contacting the Trust's IT Department.

#### **d. Off-site and Remote Working**

**Medical Records can only be transferred between Trust sites using Trust Transport, ambulances and, at WSFHT, authorised taxis.**

Medical Records may only be taken off-site if absolutely necessary and on approved business, as authorised by the Head of Medical Records or their agreed Deputy. All movement of Medical Records must be tracked on the Patient Administration System (PAS). Please see the Health Records Policy on the Intranet.

Other PCD may only be taken off-site if absolutely necessary and on approved business, as authorised by an approved departmental manager. Guidance on best practice is available from the

IG Team, and includes that a Standard Operating Procedure be in place, agreed by management, as to what the process is. These must include that:



- Information must be kept secure. This aligns the process with **GDPR** Principle 6. In relation to manual information, this would ideally mean in a locked container that does not obviously contain PCD during the transit and while in use. In relation to electronic information, the advice elsewhere in this *Handbook* must be adhered to.
- Information must not be left unattended.
- If stopping, for example to purchase fuel, information must be locked away out of sight when paying, ideally in the boot of the car. The car itself should also be locked.
- PCD should ideally not be taken home overnight. Where this is absolutely necessary it must be agreed in writing by their IAO.
- A list of the records taken offsite must be retained at base.

#### **e. Abuse of Privilege**

It is **strictly forbidden** for staff to look at, seek or share any information relating to themselves, their family, friends, acquaintances or colleagues unless they are directly involved in their care or processing the information as part of their responsibility as an employee.

**Seeking out or looking at information, or offering to sell information, is an offence under Data Protection legislation and may attract disciplinary action that could result in dismissal.** This applies to both patient and staff information.

Trust IT systems have an audit facility that monitors access to information held on that system, including 'read only' access. **You may face disciplinary action if you are found to be accessing information that is not related to your role without good reason.**

#### **f. Disclosures**

You may, as part of your job, legitimately need to disclose PCD to others:

- Keep the amount of information disclosed, even within the NHS, to a minimum.
- Do not duplicate records, on paper or in a computer, unless absolutely essential.
- Advise those to whom you are legitimately disclosing PCD that they must not pass it on.
- Ensure when PCD is disclosed to a non-NHS organisation that an agreed Information Sharing Agreement (ISA) is in place when necessary (see Chapter 25). If in doubt, contact the IG Team.

#### **g. Patient Contacts and Patient Details**

Unless you have agreement from patients to do so, do not leave messages that contain PCD on home answering machines as it may not be picked up by the person for whom the message is intended.

White boards or other displays that contain PCD should not be visible to the public.

Any notes containing PCD written whilst taking a phone call or other message must be confidentially destroyed.

## h. Safe Haven Post Process

- Confirm the name or job title of the recipient, department and full postal address.
- Ensure you address the envelope accordingly.
- Seal the information in a robust envelope.
- Mark the envelope “Private and Personal – Addressee Only”.
- If necessary:
  - Send the information by Recorded Delivery.
  - Ask the recipient to confirm receipt.
- Ensure recipient confidentiality is not compromised by unnecessary (clinical) information showing in the envelope window.
- Ensure that only the correct letter / document / information is in the correct envelope.

## i. Internal Mail

- If using internal envelopes, ensure all previous location information is fully crossed through **on both sides** (failure to do so often leads to mail being misdirected), or use a standard envelope.
- Ensure envelopes are fully addressed with an individual’s name, department, hospital / site, and a building, if necessary.
- Do not assume that all hospitals and healthcare sites receive internal post deliveries from the Trust, check with the Post Room before putting PCD in the post.
- Do not put any information in the internal post that is not in an envelope.
- Ensure information that is for a specific individual is marked ‘Private and Confidential’.
- Ensure that only the correct letter / document / information is in the correct envelope.



## j. Hoax Calls and Phishing Emails

The Trusts sometimes experience calls being received pretending to be from either internal departments or external companies, trying to obtain information from the Trust about members of staff.

Some calls sound like they are being made from call centres but the caller usually claims to be working on behalf of the Trust and is allegedly calling from departments within the hospital itself.



Some examples of the reasons that the hoax calls are being made have included Hepatitis B audits, Hep B status of locum consultants, research on Hep B status of clinicians and Health & Safety.

When asked for their contact number or email address, the callers often try to provide a reason why they cannot supply these details, e.g. they are new and do not have email/telephone extension yet. They then often try to pressurise the member of staff into giving out the information saying they need it urgently.

The advice that staff must follow is to:

- Ask the caller for a verifiable landline number on which to call them back. If they are calling from a genuine organisation they will not object. Do not accept reasons why only a mobile / direct dial number can be provided. It must be a call that goes through a company switchboard. If a verifiable number cannot be provided, treat the call as fraudulent. Or

- Discreetly transfer the call through to the IG Team. Inform the caller you will put them through to someone who can help rather than through to the IG Team as, if a hoax call, the callers tend to terminate the call at this point. Remain on the line to alert the IG Team that a suspected hoax call is being transferred.

If the enquiry is about specific member of staff, information must not be released. Instead, attempt to obtain a number that the caller can be contacted on and pass this to the member of staff being enquired about, who can respond or not as they see fit. If the call is genuine there will not be a problem obtaining a contact number.

Members of staff at the Trust have also received potentially hoax / suspicious emails from various sources, into their Trust email accounts, that instruct the recipient to either click on a link or open up an attachment.

If the recipient were to either click on the link or open up the attachment, it is more than likely that a virus/malware will be downloaded onto the computer.

These emails usually come from genuine email addresses, that could have potentially been victim themselves to a virus and there is not much that IT can do to prevent these actually arriving into staff inboxes.

The Trust's antivirus software should remove the attachments and links out of the emails but the advice to staff is that if they have any suspicions about the email, especially if it is one that is not expected or if it is from a company that they have not had any dealings with, just delete it and then remove it from the deleted items folder. Sometimes emails that look genuine may be hoaxes, and look correct, but for example may have one letter missing or replaced. Do not respond to the email or open attachments.

You must always take care when opening email attachments, especially for example if you receive a message with an attachment and believe it to be genuine on first glance. Always double check especially if it is from an untrusted source.

**If you suspect an email that you have received is a phishing email:**

- **Please do not forward it to IG or IT as this may pass any viruses in the email further around the organisation.**
- **Delete the email from your inbox, and then delete it from your Deleted Items.**
- **Let IT know by contacting the IT Helpdesk.**

#### **k. Checking Identity**

It can be difficult to strike a balance between maintaining confidentiality and ensuring the appropriate flow of information. However, it is essential that staff do not inappropriately disclose patient details in situations such as telephone calls or during the booking in process.

To ensure you are speaking to the patient, or authorised individual it is important that a three-point identification check is undertaken, as you would be asked to do if you called your bank. Checking whether any patient alerts are present will further assist in maintaining confidentiality. Doing this demonstrates that you have made best endeavours not to release to the wrong person. Should there be a discrepancy between the details provided and what is recorded on PAS, follow local guidance provided in your department. This could include writing down the 'new' information provided, leaving PAS unchanged while checking with a nominated member of your team.

If a case is particularly sensitive, contact the IG Team for advice. It is also good practice to see whether there are any alerts on the system prior to releasing any information.



Examples of the three points of identification that could be asked include, but are not limited to full name, DoB, GP, first line of address, postcode, next of kin, NHS number or date of last clinic attended.

## I. The Two Second Rule

A simple piece of advice when transferring PCD is to observe a Two Second Rule: just take two seconds to ensure:



- The right letter is in the right envelope.
- That information relating to another patient has not been picked up in error.
- No PCD other than the name and address are visible through the envelope window.
- The correct email address appears in the 'To' field.
- Emails that are meant to be sent blind to multiple recipients have the addresses placed in the 'BCC' (Blind Carbon Copy) field; this shields the full distribution list from all of the recipients.
- The correct fax number has been selected.

**To prevent the issue of selecting email addresses you no longer use, some good housekeeping advice is to regularly delete them from your address book by regularly clearing the AutoComplete.** This can be done in Outlook by:

- Clicking the File menu and selecting Options.
- Clicking the Mail window tab.
- Scrolling down to Send Messages.
- Clicking the Empty AutoComplete List button
- Clicking Yes to the confirmation window.

The impact of not double-checking before sending can be massive to the Trust. For example a member of staff from the 56 Dean Street Clinic, part of Chelsea & Westminster NHS Foundation Trust, sent an email newsletter to 800 HIV patients, accidentally putting all of the email addresses in the 'CC' rather than 'BCC' line of the email. As a result all 800 recipients received the names and email addresses of the other recipients, breaching Data Protection legislation as it inappropriately shared the most sensitive of information. They were fined £180,000 by the ICO.

## m. Confidential Waste and Confidential Waste Bins

Any confidential information, whether PCD or business information, written / printed on paper that is no longer required must be placed in a confidential waste bin.



For queries regarding the collection or disposal of confidential waste, please use the contacts in Appendix 1.

## Chapter 5: Social Media and the Use of Mobile Phone-based Messaging Apps

Social media has become a worldwide phenomenon. According to statistics website Statista, the UK's most popular social networks in 2019 were **Facebook, WhatsApp, YouTube, Twitter and Instagram**. On a general level, some simple advice, to keep yourself safe is to **never**:

- Make friends with people of whom you are unsure.
- Reveal PCD, including photos, about patients or colleagues.
- Moan about your employer, patients or colleagues.
- Discuss sensitive information.
- Upload compromising photos of yourself.



Plus, be extra careful if mixing work and private life on social media.

More specifically, messaging apps are useful and efficient if used correctly, and there is full encryption in place. However, apps such as WhatsApp, have many concerns, as information sent is backed up on the user's unencrypted cloud-based storage.

Additionally, if a member of staff leaves the organisation they can take PCD with them, meaning there is no organisational ownership of data that has been sent, which raises significant Data Protection concerns.

There is also the issue that many apps are owned by technology organisations that are not, based on recent news stories, renowned for placing their privacy and Cyber Security as a high priority.

However, this is the twenty-first century and messaging apps, such as WhatsApp, are here to stay and their benefits are great if used appropriately when needing to communicate speedily, such as for the filling of rota gaps, or during major incidents. **But what is appropriate?** It is more than acceptable to use messaging apps, such as WhatsApp, for business purposes such as those just mentioned, along with group planning and education. However:

- They must not be used as a work around for healthcare referrals / advice within or between organisations.
- The inclusion of PCD of any sort is unacceptable.

However, in urgent situations NHSx has stated that it is acceptable to use off-the-shelf applications 'where there is no practical alternative and the benefits outweigh the risk'. Generally this would mean in an emergency situation only, and where a patient's health would be in extreme risk if it were not used.

Advice and guidance is available from the IG Team as to what is considered appropriate.

## Chapter 6: Parental Responsibility

It is essential to be able to demonstrate who has Parental Responsibility whenever a child is being treated or information is being shared about them. It is important that this is able to be demonstrated, should the decisions or sharing be challenged at a later date.

Parental Responsibility is defined in law by the **Children Act 1989** as all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and their property.

People with parental responsibility are entitled to have a say in major decisions about the child such as:

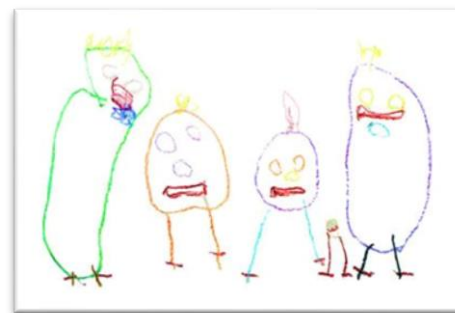
- Where the child should live
- Where they should go to school
- What religion they should practice
- What name they should have
- Giving or withholding of medical treatment
- Dealing with their money or property

Parental responsibility lasts until the child reaches 18 or marries between the ages of 16-18.

### a. Who has Parental Responsibility?

Individuals have parental responsibility automatically if they are:

- The biological birth parent of the child (legally 'mother');
- The biological parent (legally 'father') of the child, and
  - Were married / in a civil partnership with the birth parent at the time of birth, or
  - Married / entered into a civil partnership with the birth parent after the birth;
- The adoptive parents once an adoption order has been made.



Both biological parents continue to have parental responsibility even if they divorce or legally separate.

**Unmarried biological parents** did not have the same rights and responsibilities as married biological parents until the **Adoption and Children Act 2002** came into force on 1 December 2003. This is not retrospective and therefore:

- **Children born before 1 December 2003**, unmarried biological parents (legally 'fathers') can only get parental responsibility by:
  - Obtaining a parental responsibility order via the courts, or
  - Completing a Parental Responsibility agreement form with the birth parent (legally 'mother') of the child and taking it to a solicitor.
- **Children born on or after 1 December 2003**, unmarried biological parents (legally 'fathers') automatically have parental responsibility if they are named on the child's birth certificate.

**Children conceived by artificial insemination:** if the child was conceived through artificial insemination on or after 6 April 2009 and the birth parent (legally 'mother') is in a civil partnership or married at the time of the birth, then their civil partner or spouse will automatically have parental responsibility for the child. Both names should be added to the birth certificate. Unmarried partners will have parental responsibility if the child is conceived through a UK-licensed fertility clinic and the required consent forms are signed at the clinic. This applies to same-sex and opposite-sex couples.

### b. What About Non-Biological Parents?

Other people can also acquire Parental Responsibility for a child. More than two people can have parental responsibility for the same child. These might include step-parents, grandparents or same-sex partners. Non-biological parents can acquire Parental Responsibility in any of the following ways:

- **Married step parents and civil partners acquire Parental Responsibility for a step child or child of the family by either entering into a Parental Responsibility agreement or by asking the court to make a Parental Responsibility order.** Parental Responsibility agreements require signed consent from all parents with Parental Responsibility.
- **They adopt the child** – when an adoption order is made the adoptive parent or parents gain Parental Responsibility for the child and the biological parents **lose** it. If the adoption is a joint adoption between a biological parent and their partner, the person they are adopting with gains Parental Responsibility and any other person who had it loses it.

- **They are appointed as a guardian of the child** – a person or persons with Parental Responsibility can appoint another person or persons to be the child's guardian after their death. The appointment can be made in writing (and must be signed and dated) or in a will. The appointment of a guardian will only take effect if:
  - There is no other person with Parental Responsibility for the child, or
  - If the parent who made the appointment was named as the person with whom the child lives in a child arrangements order at the time of their death and the surviving parent was not also named as a parent with whom the child shall live; or
  - If the parent who made the appointment was the child's only special guardian.
- **The court makes a child arrangements order stating that the child is to reside with them** – in this situation the named person will acquire Parental Responsibility (if they don't already have it). They will have Parental Responsibility for the duration of the child arrangements order but would lose it if the order is brought to an end by the court.
- **The court makes a special guardianship order** – when the court makes a special guardianship order in favour of a non-parent, this person or persons will acquire Parental Responsibility for the child. The order provides the child with a legally secure family home but unlike adoption the parents **do not lose** Parental Responsibility. A special guardian, however, can overrule the Parental Responsibility of the parents when making decisions about the child.
- **Local Authorities can acquire Parental Responsibility for a child if the court makes a care order, emergency protection order or interim care order in respect of that child.** The Local Authority will then share Parental Responsibility with anyone else who has Parental Responsibility for the child but the Local Authority can overrule any decisions that they do not feel are in the child's best interests. The child then becomes a 'Looked After Child'.

### c. Proof of Parental Responsibility

To enable someone to prove that they have Parental Responsibility they need to provide proof of their identity (e.g. passport, their birth certificate and photo ID) together with a copy of one of the following documents:



- The child's Birth Certificate – To acquire Parental Responsibility the biological parents must have registered the child's birth together on or after 1 December 2003, or
- Marriage Certificate, or
- Civil Partnership Certificate, or
- Parental Responsibility Agreement entered into by biological parents, or
- Adoption Certificate, or
- Copy of a Court Order giving Parental Responsibility

### d. Consent from People with Parental Responsibility

In cases where a child is unable to give informed consent themselves, people with Parental Responsibility are entitled to give consent for medical treatment on their behalf. There are limits on what parents are entitled to decide and they are not entitled to refuse treatment which is in the child's best interests. Staff should take further advice, as appropriate in their area of work, and / or refer to the **Consent Policy** on the **Intranet**.

### e. Legal Liability Guideline Statement

These guidelines are considered to represent best practice. Staff may exceptionally depart from any relevant Trust guidelines providing always that such departure is confined to the specific

needs of the individual circumstances. In healthcare delivery, such departure shall only be undertaken where, in the judgement of the responsible healthcare professional it is fully appropriate and justifiable. Such decisions must be fully recorded in the patient's Medical Record.

## Chapter 7: Use of Childrens' Information

The question often arises as to at what age children can make decisions about the use, access to and sharing of their own data. There are no strict rules on this in England, so it is advisable that decisions are taken on a case by case basis based on various factors, including their relationship with their parents or guardians and whether, for example, they have a learning disability. However, there are some indications that points in the direction that, as a rule of thumb, **children are able to make decisions about how their own information is shared or accessed from the age of thirteen**. This is based on three factors:

- **DPA18** says that children can make their own decisions to access information society services, i.e. internet based services, from the age of 13. This is the only place in any Data Protection legislation that an age is specifically given.
- Scotland presumes children of 12 or more are able to make their own decisions regarding the use of their data.
- The concept of **Gillick competence**, although undefined as a specific age, that a child may make their own decisions if they have sufficient understanding and intelligence to understand what is being proposed.

The age of 13 has, however, never been tested in Court, this is simply a practical application of several indicating factors to help facilitate the making of appropriate decisions.

## Chapter 8: Subject Access Requests



Under the **GDPR**, all living individuals have the rights outlined in Chapter 3, which includes access to their information, generally known as a Subject Access Request (SAR).

Requests for copies of Medical Records are dealt with by specialists within the IG Team, who ensure they are dealt with in line with the statutory requirement of one month. The Trust has robust SAR guidance with agreed procedures to ensure each request receives prompt attention.

Most of the information released about patients tends to be in paper Medical Records or electronic systems, but **staff must be aware that absolutely anything they write about a patient, wherever it is stored, could be released when a request is received, as all information technically forms part of their wider Medical Record**.

**This includes information about them written in, for example, a diary, on a Post-It note, in emails or on a scrap of paper stored in a drawer. Increasingly there have been requests for all emails concerning individual patients.**

SARs may be received in other areas of the Trust, including Human Resources, Estates, Research & Innovation, Radiology and Occupational Health. They should have local procedures and representatives to deal with requests. Requests for images captured on CCTV are, like other records, managed through **GDPR**. If a request is received and you do not know how to deal with, contact the IG Team for advice.



Some limited people are also able to access records of the deceased under the **Access to Health Records Act 1990**. Please contact the SAR Team for advice on this.

For queries regarding any aspect of SARs, please contact the team as detailed in Appendix 1.

## Chapter 9: Management of Clinician to Clinician Handover Sheets



To provide a safe and confidential service to our patients it is necessary, pending an electronic solution, for clinicians to work from paper lists of PCD. It is vital these lists are handled and disposed of in a secure and confidential manner when no longer required in order to protect patient information.

### a. Definition

The term Handover Sheet is used here as a broad term for any list of patients used for the purpose of tracking and delivering patient care. They include, but are not limited to:

- Clinician to clinician handover lists.
- Ward round lists.
- Ward handover reports.

### b. Maintaining Confidentiality

**The use of paper lists of patient information represents a significant risk in terms of data breaches should they become lost or misplaced and it is therefore very important that staff continue to adhere to this guidance.**

To reduce this risk, staff must:

- Distribute paper lists of patient information only to the limited members of staff for whom there is a clear need for them to have it to provide safe and effective patient management.
- Ensure that only the minimal numbers of lists required are produced.
- Ensure that the format of the information does not risk compromising patient confidentiality, i.e. by using only the minimum essential information required for safe patient care.
- Not include social / safeguarding details (if necessary details must be held separately in a well-controlled restricted access list).
- Avoid folding lists and placing in pockets / bags.
- Not remove lists from wards; they must be put in a designated place for later retrieval. If there is no alternative but to move list between wards, folders must be used.
- Update patient information onto electronic systems before leaving the area.
- Always dispose of paper lists securely in confidential waste bins provided in all areas at the end of each shift. It is the responsibility of each member of staff to do this. Further information regarding confidential waste bins is in Chapter 4.
- Not record handover details on personal mobiles or other personal hand-held devices. **This is strictly prohibited.**
- Not record PCD in personal notebooks that are then taken out of the Trust. This is strictly prohibited; any such pages must be disposed of in the confidential waste. It is understood that trainees and non-trainees may need to keep a personal log. This must be maintained through the appropriate Professional College or School e-portfolio, following its formal advice.
- Follow the Caldicott Principles (see Chapter 3).

### c. Identifiers

A review of the format of documentation following a number of data breach-type incidents determined that patient identifiers **must** be limited to those considered essential for the reliable and safe identification of patients. Therefore **only** the following identifiers are permitted:

- Ward
- Date of admission
- Lead Consultant
- Bed Number
- Initials, or patient's first name and initial letter of surname
- Age (not DoB)
- Hospital or NHS number to allow verification and access to electronic information

### d. Accountability

All staff producing paper patient information lists will be held accountable for ensuring that:

- Documentation is compliant in terms of patient identifiers.
- Each page of the paperwork contains the name of the user.
- Paperwork is kept secure at all times and is disposed of in confidential waste.

Any loss of documentation is reported immediately to the relevant line manager and reported onto Datix, the Trust's incident reporting system.

## Chapter 10: Sharing Personal Information with the Police

Under the law, no matter what is shown on television dramas, the **Police and other law enforcement agencies do not have automatic right to see PCD about patients or staff**, although the Trust does its best to cooperate with them when it is legal to do so.

When requests are received, even with a Police Officer in attendance, each one must be dealt with based on its own merit; PCD must not be released without careful consideration.



On receipt of a request from the Police, the Officer must be requested to complete a **Police Personal Data Request Form**, which can be found on the **Intranet**. Alternatively the Police may use their own similarly named form.

**Most requests are unlikely to be urgent, so should be passed to the IG Team to process during office hours.** If they are received out of hours, and are considered urgent, they should be passed to the Site Manager to assess how to deal with them.

Scenarios where the Police may be requesting information and it could be considered urgent for a current investigation may be murder, manslaughter, rape, treason, kidnapping, child abuse, serious harm to state security, serious harm to public order, as well as crimes involving substantial financial gain. This is not a complete list, nor will all of the scenarios always require urgent attention.

In many cases the IG Team, along sometimes with the SIRO and / or Caldicott Guardian, will make the decision to release to the Police. However, unless there is a legal basis to do so the Trust does not always have to, and makes decisions based on a public interest test.

## Chapter 11: Information Governance and Cyber Security Breaches

Each member of staff has the responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way. In September 2018 NHSD released updated guidance on how Data Security and Protection incidents should be graded. Entitled the *Guide to the Notification of Data Security and Protection Incidents*, this guidance is in line with the **GDPR** and uses a standard Information Security Classification as to whether incidents are personal data breaches of:



- **Confidentiality** – i.e. it has been made available or disclosed to unauthorised entities.
- **Integrity** – i.e. the accuracy and completeness of information has been compromised.
- **Availability** – i.e. the data is not accessible when required by authorised personnel.

Staff must always think carefully before sharing PCD and report on Datix, the Trust's incident reporting system, any IG incident of concern.

**It is better that a potential personal data breach is reported and downgraded later, rather than not reported and becoming more serious by not being known about.**

It is essential that incidents are robustly investigated so that lessons can be learned from them, both within the team where they occurred and to the benefit of the Trust as a whole.

If ever information is sent to the wrong destination, it is important that the Trust attempts to recover the documentation that has been disclosed in error to aid investigation and to ensure confidential destruction when appropriate to do so. Sometimes the recipient of the information may not be willing or able to return it by post or in person and, if logistically feasible, it is entirely appropriate that someone from the Trust collects it. Ideally this would be someone from the department that mistakenly disclosed the information in error.

If in any doubt regarding the reporting or management of IG and cyber security incidents, ask your line manager, or the IG Team who may pass the query to the SIRO and / or Caldicott Guardian.

The implementation of the **GDPR** has brought with it a new regime around incident reporting. This creates two new obligations: the mandatory reporting of serious personal data breaches and the need for a Duty of Candour where the breach is likely to result in a high risk to an individual's rights and freedoms.

### **a. Mandatory Reporting of Serious Personal Data Breaches**

This must occur when a personal data breach is likely to result in a significant risk to the rights and freedoms of the individuals concerned. These include:

- Loss of control over their personal data.
- Limitation of Data Protection rights (see Chapter 3).
- Discrimination.
- Identity theft or fraud.
- Financial loss.
- Unauthorised reversal of pseudonymisation.
- Damage to reputation.
- Loss of confidentiality of personal data protected by professional secrecy.
- Any other significant economic or social disadvantage.

If such an impact is believed to have taken place, the Trust must notify the ICO within 72 hours of becoming aware that a serious personal data breach has occurred. Time is therefore of the essence when reporting incidents onto Datix to enable investigation to determine whether the incident has reached the threshold for notification.

An organisation is permitted to notify the initial findings to the ICO and then provide additional information as the investigation progresses.

**Fines for personal data breaches can, in principle, be as high as 4% of the organisation's turnover, or €20m, whichever is higher.**

In addition, organisations that fail to report a personal data breach when they should have done can be further fined 2% of turnover or the equivalent of €10m, whichever is higher.

### **b. Mandatory Duty of Candour**

Where a breach is likely to result in a **high** risk to an individual's rights and freedoms, the Data Controller (i.e. the Trust) must undertake a Duty of Candour using clear and plain language, including:

- An explanation and apology (in writing) in relation to the breach.
- Contact details for the DPO.
- Possible consequences of the breach.
- How the Data Controller has mitigated the breach.

Generally the Duty of Candour must be undertaken by the Department with responsibility for the process / activity where the personal data breach occurred, potentially with the guidance of the IG Team.

## **Chapter 12: Decommissioning Work Areas: Checking for Confidential Information**

From time-to-time it is necessary to close down buildings, wards and other work areas, either temporarily or permanently. When doing so it is important to check that no PCD for either patients or staff is left behind, as occurred with Belfast Health Trust.



It was fined £225,000 by the ICO in 2012 for failing to secure confidential files at Belvoir Park Hospital, which had closed in 2006. The PCD of many thousands of patients was involved, including Medical Records, x-rays, scans and laboratory results. It also involved 15,000 staff records, including unopened pay-slips.

To help prevent such issues the Trust have a Decommissioning Checklist to be completed by any service that is vacating an area of work, which is available on the **Intranet**. It is a structured checklist to support the Manager of the area to ensure no PCD is left behind, and that all patient and staff information is moved to a secure area. It also reassures the Manager of the area as it guides them to take photographs of the areas when they are clear and to sign that they have personally seen it cleared.

It is the responsibility of the management team organising the move to ensure this checklist is completed.



Once finalised it must be stored by the Manager of the area as evidence that they completed a full check of the area to ensure no PCD remained once their Team had vacated.

## Chapter 13: Monitoring Access to Personal Confidential Data



Staff use of electronic systems which access, process or transfer PCD is monitored and audited. Where care records are held electronically, audit trail details about such access to a record can be made available to patients concerned upon request.

**Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with disciplinary procedures.** In addition, unauthorised disclosure of PCD is an offence and could lead to criminal prosecution.

Similarly staff accessing their own data is considered misconduct and an abuse of privileged access to that information by virtue of their job, and could result in the same action. Any need for staff to see their own data must be requested as a SAR (see Chapter 8).

## Chapter 14: Information and Cyber Security

Information and Cyber Security is not solely related to IT and computers, in many ways it reflects the whole of IG covered in this *Handbook*. It concerns every member of staff doing their utmost to maintain the Confidentiality, Integrity and Availability of patient and staff information, to ensure it is available to the right people at the right time.



With such reliance on electronic data systems, and with the portability of data that comes with it, come new vulnerabilities to cyber security risks. There have been several high profile cyber-attacks and incidents against various organisations including the “WannaCry” ransomware attack against one-fifth of NHS Trusts in May 2017.

Another example is a computer virus that affected the Northern Lincolnshire and Goole NHS Foundation Trust in autumn 2016 for five days, meaning that thousands of routine operations and outpatient appointments had to be cancelled. This was because the virus caused the computer network to crash.

In addition to this sort of disruption, it has been suggested that a person’s Medical Record is much more valuable than credit card numbers on the black market.

**Some very basic principles to support this in healthcare include:**

- Ensuring patients’ and staff information is not left unattended.
- Maintaining a clear desk policy when away from your workstation.
- Locking cabinets and drawers containing confidential information.
- Securely storing NHS Smartcards.
- Securing key-padded rooms.
- Wearing ID badges.
- Not leaving confidential papers or waste lying around.
- Locking PCs when not using them.
- Not writing passwords down.
- Not installing or download software onto Trust computers.



**It is not a breach of data protection legislation to display a name badge containing a member of staff's full name at a place of work, and it is in line with the "Hello my name is" initiative established by the late Dr Kate Granger MBE. It is appropriate for those with whom staff have interaction to know who they are communicating with and by whom they are being treated.**

Without effective Information and Cyber Security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the Trust, therefore the organisation must ensure that the information is properly protected and is reliably available.

- Access to all PCD whether held on paper or electronically must be restricted.
- Staff must ensure that security doors are closed properly and blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team or it is suspected that someone else knows the code.
- All staff must wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access. Visitors should be met at reception points and accompanied to appropriate member of staff or meeting and also should be asked to sign in and out of the department.
- On termination of employment or contract staff must surrender door keys and all relevant Trust equipment as part of the staff leavers' process.
- All computer assets including hardware and software must be recorded on an Information Asset Register that details the specification, user and location of the asset.

All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. The organisation will investigate all suspected and actual security breaches.

#### **a. Protecting the Trust and Its IT Network**

Some things the Trust's IT Team do to ensure systems remain secure, and to support staff, include:

- Restricting the installation of potentially suspicious files.
- Regularly updating computers to protect against system vulnerabilities.
- Ensuring computers are routinely monitored for viruses, and that anti-virus software is in place.
- Having an email filtering system to "catch" suspicious emails before they reach the end user.
- Protecting the network borders with firewalls to restrict access.
- Only allowing the use of encrypted memory sticks.
- Actively monitoring the network and all devices that attach to it, for vulnerabilities and unauthorised software.

To support this, all staff must:

- Not share usernames / passwords with anyone, including line managers and IT.
- Update their passwords regularly and keep them complex by using a combination of upper and lower case letters, numbers, and special characters (such as question marks and exclamation marks).
- Not subscribe to non-work related email subscriptions with work email account.
- Not follow links or open attachments from an unrecognised sender.
- Ensure any changes to your IT systems are only completed with IT authorisation.
- Ensure they report any suspicious incidents or faults to IT immediately.
- Ensure they report any suspicious emails, taking care not to click on any links etc.

## **b. Remote Working and Portable Devices**

Developments with IT have enabled authorised staff to adapt to more flexible and effective working practices; a small number of staff use these for essential business purposes. Although these working practices are advantageous, it is important for users to understand the associated risks, and ensure that information accessed remotely or held on portable devices, is protected by adequate security.

Staff are responsible for the security of any portable devices issued to them, and should take all necessary precautions to avoid loss, theft or damage. Should this occur it should be reported on Datix to your line manager at the earliest opportunity.

Encryption is mandatory in all Trust issued mobile devices used to store PCD.

Any portable computing device is an attractive item and must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, or any PCD, ensure that it is safely stored out of sight.

You must not leave the device unattended for any reason unless the session is 'locked' and it is in a safe working place, devices must not be left in an unattended publically accessible room for example.

Ensure that other non-authorised users are not given access to the device or the data it contains.

With regard to USB / portable computing devices:

- All USB / portable computing devices, including memory sticks, must be encrypted.
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available.
- Information must not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible.
- You must ensure that any suspected or actual breaches of security are reported onto Datix.
- Staff leaving the organisation or no longer requiring use of an organisation's procured device must return the device to their line manager.
- You should not under any circumstances use any mobile device whilst in control of a vehicle without an approved hands free kit.
- You must retain an awareness of your surroundings when using a mobile device, especially when discussing confidential information.



It is Trust policy to never transfer PCD unless there is no alternative and only then if the memory stick is a Trust approved encrypted device and you are authorised by your Line Manager. Ask yourself, could the data be stored / transferred using Trust network folders? Only transfer the minimum amount of identifiable data. Data held on encrypted memory sticks is secure as it can only be accessed by means of a password. Without the password these devices are useless therefore you must always keep the password separate from the device in a disguised format so it cannot be easily identified and never attach the password to the memory stick. If the memory stick is lost or stolen you will lose any data on it so please ensure you have a secure back-up on the Trust network. It is good practice to keep a note of what information is held on the stick and remove it as soon as practically possible. Information transferred in this way must not be copied from the sticks to non-Trust owned equipment.

Unencrypted memory sticks do not have built in security and should one be lost or stolen, potentially anyone could plug it into another computer and access all the data. For this reason you will not be able to use an unencrypted memory stick in most Trust computers to download any information. Only Trust owned approved devices are permitted.

There are certain risks in the use of memory sticks; they have the following features but care must be taken with them as they can easily be lost due to their very small physical size:

- Their size makes them easily portable, e.g. in a pocket or on a key ring.
- They weigh next to nothing but can hold a lot of data.

Trust-issued encrypted memory sticks will work in almost all Trust computers that have a USB socket. Memory sticks must only be used on Trust computers with active, up to date and on-access scanning anti-virus software.

If you intend to take Trust owned devices off site, you must seek approval from your manager.

These guidelines are intended to complement, but not replace the Trust's formal policies and procedures regarding Information Security. The latest Information Security documents, policies and leaflets are available for download from the IG Page on the **Intranet**.

If your stick is lost or stolen please report it on Datix.

### **c. Destruction and Wiping of Removable Media**

If you have removable media for destruction, such as CDs, that you believe may contain PCD, you must request hessian sacks from the Porters and clearly label them as "Portable Media for Destruction". When the sack is half full the Porters will remove it for you upon request.

If the memory stick is to be given to another user or department the device's contents must be wiped before it is handed over.

### **d. Use of Secure Print**

When printing from networked secure printers, it is key that care is used.

Most staff use their Smartcard or Trust ID badge to retrieve printing; however, a limited number of staff necessarily use a PIN code. If such a code is used it is essential that it is typed in correctly, as failure to do so means it is probable you will print documentation that will not belong to you, and may contain PCD that you are not entitled to see.

## **Chapter 15: Use of Email**

Email is used by virtually everyone within the Trusts to communicate with colleagues, as well as communicating externally with other colleagues in the extended NHS, social care and other sectors. There are some basic guidelines to ensure that it is used effectively, safely, and does not breach IG rules. Some other elements regarding email are covered in Chapter 4.

### **a. Sending Confidential Information Securely**

For internal communication we use the @nhs.net email domain (often called NHSmail).

## To send secure internal email:

It is secure to send from name@nhs.net to name@nhs.net.

It is possible to send a secure email to non NHSmail addresses providing **[secure]** is typed in the subject line. It is important that it is spelt correctly and is in square, rather than rounded, brackets. Behind the scenes NHSmail will work out if encryption is needed, users no longer need to check if the email domain of the recipient is secure. NHSmail is a secure service which enables the safe exchange of sensitive and patient identifiable information between different types of email account when using **[secure]**.

### b. Auto-Forwarding of Email

Staff are not permitted to set auto forward rules on their mailboxes to any other destination, as this can result in data being sent insecurely and potential breaches of Data Protection legislation.

### c. Managing Emails as Records

Emails can be, and often are, formal business records which provide evidence of important transactions. This highlights the need to manage emails as records. An email record must be managed according to content and not based on the fact that it happens to be an email. **It is every staff member's responsibility to do this regularly and effectively.**

Given the volume of emails sent and received each day it is neither practical nor desirable to manage each and every one as a formal business record. The skill is to be able to identify and capture that small percentage of emails that need managing as records. This can include those which deal with or contain:

- Information which needs to be retained for compliance reasons e.g. as part of a medical record or business audit trail.
- Formal agreements, e.g. approval of contracts, project plans, policies.
- Decisions / confirmation of actions, e.g. approval to spend money or carry out an activity.
- Confirmation of completion, e.g. project sign off, receipts of goods etc.

For those emails which are identified as being records it is important that they are managed in context with the other records to which they relate, i.e. transferred from the user's inbox to the appropriate storage location, which could include either printing it and storing it in hard copy, such as in a Medical Record, uploading to an electronic record, or saving it to an appropriate network folder.

To ensure authenticity and completeness it is important that all sender and recipient information is carried over with the email record, including all parties receiving the email as a carbon copy (CC) or blind carbon copy (BCC).

To ensure integrity it is important to ensure and be able to demonstrate that no element of the email has been or can be altered in any way after being saved as a record. This includes changes to the content, but also to the transmission data and the content of any attachments transferred with the original message. This may be variously achieved by altering the properties of the file to a 'read only' status, or modifying the permissions within the specific area of the record keeping system to prevent further amendment.

Chapter 20 also explains how information in email can and should be released following a request under the **Freedom of Information Act 2000**.



#### d. Emailing Patients

You should not normally use email to establish a patient-clinician relationship. Rather, email should add to and follow other, more personal, encounters, when the patient has given permission for you to communicate with them by email.

When writing down an email address, take time to ensure that it has been noted correctly, for example, avoiding misspellings of names such as Clare/Claire, ensuring any numbers in the address are accurate, and that the correct domain name (such as Gmail, Yahoo!, Outlook etc.) are used. Sending a test email is a good idea to ensure the address is correct before sending PCD.

Only use email with patients and service users who have given their informed consent for using email to communicate with them. This consent should be clearly recorded in their Medical Record.

Even when using secure email, privacy and confidentiality can be broken, usually as a result of human error. Patients should have the opportunity to accept this risk before you send any PCD by verbal discussion followed by a test email prior to emailing.

If a patient has particular accessibility requirements, you should explain locally available options and, if possible, demonstration systems or training should be provided beforehand. Accessibility refers to the design of products, devices, services, or environments for people with disabilities. Accessible design makes sure a patient can have both direct access (in other words without any help) and indirect access meaning compatibility with a person's assistive technology (for example, computer screen readers).

Some issues should never be discussed via email without the specific agreement of the patient. For example, this may include, but is not limited to, treatment concerning mental-health or sexual-health diagnoses.

## Chapter 16: Photography and Recordings

#### a. Photography and Recordings for Patient Care

When making any audio or visual (AV) recording of patients, care must be taken to respect patients' dignity and privacy. There must be a fully justifiable purpose for an AV recording to be carried out.

In the vast majority of circumstances, unless there is extremely good reason not to, Trust equipment must be used for any form of AV recording. There must be a clear procedure in place for use of these devices, including a user log, secure storage and deletion arrangements.

As outlined in the **GDPR** a patient's giving of consent for their information to be processed can be either verbal or written. However, even if verbal it must be recorded in the Medical Record in a similar manner to written consent, noting which of three levels of consent is being agreed to:

- Recording in Medical Record only.
- For use in education / teaching.
- For publication (for which further specific consent is required pre-publication agreeing where sating where the images will be published etc.).



## **b. Photography and Recordings for Non-Care Purposes**

It is good practice and courteous to inform staff at formal meetings that a recording is taking place (such as for minute-taking). Although explicit consent is not necessary as the staff are acting in a professional capacity.

Recordings are often taken at organised events and may be published on the internet. Organisers of events should ensure that delegates know that recordings are taking place and be given the opportunity to opt out if they wish.

If staff need to take team photographs in a clinical environment this is permitted so long as care is taken to ensure there is no risk to patient confidentiality. The use of consent forms should also be seriously considered.

Service users attending complaint / concern / feedback meetings where the recording would not form part of the Medical Record should provide consent for the recording to take place and be given assurance on the purpose for the recording, storage and retention arrangements.

Staff must seek prior consent if they wish to record other events, including 1-2-1 meetings, sickness discussions, appraisals etc. If consent is not granted, then the recording should not go ahead.

## **c. Staff Use of Personal Recording Devices**

The Trust has an obligation to provide a safe environment to deliver patient care. Staff should be aware that personal mobile phone / cameras should not normally be used for private use in areas where care is delivered and where patient confidentiality could be compromised and should therefore make use of more suitable areas such as staff rooms.

Staff must be vigilant when taking a mobile phone into care areas, even if it is not being used at the time. Incidents of inadvertent live streaming on social media have been reported.

Departments must clearly define local procedures for use of personal mobile phone / cameras during working hours.

In normal circumstances it is not permitted to take any type of patient / staff recording on staff personal mobile phones. However, in exceptional circumstances where there is no Trust-owned equipment available and the situation is time critical the recording can take place as long as a risk assessment is carried out. At BSUH before resorting to using a personal mobile phone, Clinical Photography must be contacted to ascertain their availability to take and manage the photographs.

Staff that have no option but to make a recording on their own device must upload it to the Trust network as soon as possible and ensure it is permanently deleted from the device and cannot be recovered. Auto back-up should also be switched off first. At BSUH any such images should be securely removed from the device and passed to the Clinical Photographers for upload to the Medical Image Manager system.

Recordings should not be sent over a mobile phone network to another device, nor should they be emailed outside NHSmail, transferred via instant messaging apps or published on social media.

## **d. Recording Telephone Conversations with Patients**

Some departments routinely carry out recording of telephone conversations with patients. This is for training and quality assurance purposes. Patients must be informed that calls are recorded via

an automated message, and an opt-out process must be in place for patients who do not wish to be recorded.

#### **e. Processing and Storage of Photographs and Recordings**

Visual recordings of patients should be securely stored within patients' Medical Records. If stored elsewhere, there must be effective cross reference to link the images to the correct patient's Medical Records. The storage location must be clearly identified within the Medical Record to enable effective and efficient retrieval. Recordings should not normally be stored on removable media.

AV recordings must be removed from recording devices as soon as possible after the recording has taken place. They should be processed and stored safely on a Trust secure network drive to prevent accidental loss, unauthorised viewing or damage. There must be appropriate access control to ensure only the individuals who need access for justified reasons can do so, in line with the consent level agreed.

Departments that routinely carry out their own AV recordings must have a documented local procedure which complies with the guidance in this Chapter of the *Handbook*.

#### **f. Disclosure of Photographs and Recordings**

Recordings that are made for patient care generally form part of the Medical Record and must be handled in line with Data Protection legislation for the disclosure of personal information. Therefore recordings may be subject to disclosure under the provision of Subject Access. Requests should be directed to the Trust's Subject Access Team (see Chapter 7).

#### **g. Photographs and Recordings**

All AV recordings of patients must be retained in line with the [Records Management Code of Practice for Health and Social Care](#).

#### **h. Photographs and Recordings Made by Service Users**

Staff may encounter service users using recording devices across the Trust. These are often, but not limited to, mobile phones. It is important for staff to ensure that recordings made by service users do not compromise the confidentiality of other patients or obstruct staff in their duty to provide effective patient care.

If staff witness service users making recordings, and it poses a risk to patient confidentiality, they should be advised that their actions are inappropriate and the recording deleted. Trust Security must be called for individuals who are violent, aggressive or excessively resistant.

While it is acknowledged that it may be desirable to ask patients to seek agreement from staff to make recordings, clear legal opinion has been sought by NHSx, which provides National IG guidance, that there is no legal requirement for patients to seek consent to make recordings.

Recording conversations can help reduce anxiety for patients trying to remember and understand what was said. It also allows them to share the information later with their loved ones and carers. As a matter of good practice, the patient/service user should inform the member of staff if they plan to record the conversation and out of politeness ask if it is acceptable to them.

## **i. Communication with Patients**

Service Managers should consider displaying relevant posters in their areas to clearly set out to patients expected appropriate behaviour.

## **j. Examples of Acceptable and Non Acceptable Behaviour**

Examples of potentially acceptable behaviour include, but are not limited to:

- Parent taking a photograph of their newborn baby on their own mobile phone with no staff or other patients captured in the image.
- Patient agreeing with their consultant in advance to make an audio recording on their mobile phone of their clinic appointment and then playing it back later to their partner.
- Team photograph taken to celebrate 12 months without a pressure ulcer and published on Twitter with full consent of all staff and no patients or their information visible.
- Patient requesting staff to take a photograph of them on their own mobile phone to remind them of physiotherapy exercises.

Examples of potentially unacceptable behaviour include, but are not limited to:

- Patient making a visual recording on their mobile phone of a busy waiting area and publishing it on social media.
- Patient taking a photograph of other patients in their hospital beds in a ward.
- Staff member taking a covert audio recording of a disciplinary meeting and sharing it with a solicitor.
- Covertly recording colleagues to illustrate loud conversations.
- Relative / family member taking an AV recording of a patient having treatment where the patient is clearly not providing consent.
- Staff member taking an office “selfie” with colleagues in the background and uploading to Facebook without the permission of staff captured in the image.
- A patient’s friend, partner or relative taking photos in any way in a clinical area that would detract from the patient receiving the best possible treatment.

## **Chapter 17: Video Consultations**



In 2015 the former IG Alliance released guidance on the use of video conferencing for consultations. This Chapter is modelled closely on that document, and concerns the use of applications including NHS Video Consult (Attend Anywhere), given it is a cost effective and time saving option for managing consultations, if the risks are managed appropriately.

Managing the risks associated with video consultation needs attention from both care professionals and patients and input from IG and IT staff. Technical IT solutions that are available generally offer greater security, reducing technical risks for both the organisation and patients.

Care professionals should:

- Undertake a risk assessment before using video consultation solutions for care purposes. A workshop or joint exercise is recommended to consider different categories of service users. Are there circumstances where care outcomes might be undermined by using this technology? Should certain forms of care, e.g. sexual health, be excluded? IG experts should be involved to



ensure that any risks to privacy and confidentiality are considered, e.g. confidential or sensitive matters should only be discussed in a private space (i.e. where others cannot overhear).

- Be trained to use the system and be made aware of the issues that need to be considered.
- Use their professional judgement as to whether video conferencing is a suitable form of communication with a particular patient. It may not be the best approach even where a patient is keen.
- Be aware that video consultation is unlikely to be the right solution where the matters to be discussed may cause a service user distress or anxiety, or to discuss matters of particular sensitivity, e.g. informing an individual that they have been diagnosed with a terminal illness or potentially stigmatising condition.
- Ensure that relevant outcomes are recorded within the service user's Medical Record. Video consultations should not be recorded, unless the service user provides explicit consent. If provided this must be noted in the Medical Record.
- Ensure the consulting room environment is fit for carrying out a consultation with patients.

On receipt of a request to the IG Team to use video consultation, they will:

- Support the requestor in completing a Data Protection Impact Assessment (DPIA) (see Chapter 23). This will provide assurance that use of such solutions will be secure and that the privacy of patients will be maintained. Patients must be made aware that no communication over the internet is entirely secure and should be provided with guidance on the security of the system being used.
- Advise that if you chose to use a free system, you are unlikely to have any contract in place with the provider, which means in most instances you would not have any recourse to legal action should a breach occur.
- Advise that only corporate devices with adequate security may be used.
- Advise that the request is undertaken in close consultation with the IT Department, so as to ensure that appropriate security measures are in place with the selected system, including a means to check the identity of the patient, as well as technical issues such as passwords.

## Chapter 18: Information Governance Mandatory Training



Every member of staff is required to complete mandatory annual IG training. This includes all new starters, existing staff, temporary workers, volunteers and contractors. The Trusts have a responsibility to ensure that those working with our patients' and staff information are aware of the IG principles and the risks to the reputation of the Trusts which may occur, if processes are not followed.

This requirement was emphasised in the summer of 2015, following Cambridgeshire Community Services NHS Trust being severely criticised by the ICO for not training their staff regularly enough, and training far too few of them.

The IGSG has agreed a Training Needs Analysis and identified IG training which needs to be completed by those within different job roles and functions. In summary:

- New starters must complete induction training at the Trust Welcome Day.
- Existing staff must complete IG training at one of the annual Mandatory Training Days or via one of the e-learning modules that are available:
  - At BSUH [REDACTED]
  - At WSHFT [REDACTED]

If you are reading a hardcopy of this *Handbook*, please contact the IG Team to be directed to the location of these e-learning modules.

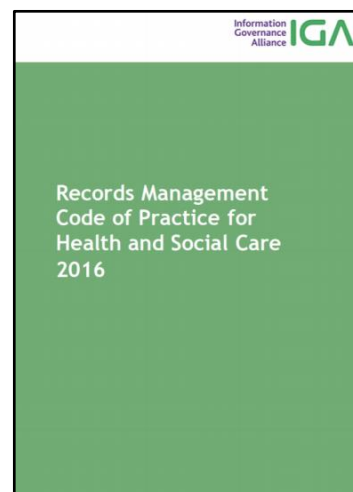
Bespoke face-to-face sessions are available for specific teams or requirements by contacting the IG Team.

## Chapter 19: Records Management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated, whether in manual / paper or electronic / IT format. This is from their creation, all the way through their lifecycle to their eventual disposal. It is the aim of the organisation to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

The NHS has at least two categories of records, Medical and Corporate / Business. Both can be either manual / paper or electronic / IT.

- **Medical Records** contain all of the patient's health information for all specialties and include, but are not limited to, private patients, x-ray and imaging reports, registers, etc.
- **Corporate / Business Records** are administrative records including, but not limited to, those for personnel, estates, financial and accounting records, and notes associated with complaints.



Records within the NHS can be held in paper (manual) or electronic form and all NHS organisations will have a duty to ensure that their patient record systems, policies and procedures comply with the requirements of the [Care Record Guarantee](#).

- Management of the Trusts' paper and manual records are guided by the [Records Management Code of Practice for Health and Social Care](#) and the **Health Records Policy** both of which are on the **Intranet**.
- To ensure the availability and known whereabouts of manual Medical Records at all times, whenever they are moved between locations, they **must** be tracked on the PAS.
- Records should be complete and accurate in order to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to protect the legal and other rights of the organisation, its patients, staff and any other people affected by its actions and provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

The following areas should be considered when maintaining records:

### Creation

- It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they have not been classified or if they have been classified inappropriately.
- It is best to restrict 'creating or deleting folder responsibility' to limited amount of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space will be required. Should a member of staff require a new folder to be created, they will need to be granted permission from the lead administrator.
- Each department should compile a list of standard terms and uniform terminology as naming conventions for files and folders.
- All electronic document storage should be kept on network drives, and not on local drives on laptops or Desktop Computers.

- Version controls should be applied and periodically reviewed.
- Records with PCD should be controlled through the use of logins, password protection and encryption

### **Naming / Referencing:**

- Keep file names short, but meaningful.
- Always give numbers as two-digits i.e. 01-99 unless it is a year or another number that requires more than two digits e.g. 001-999.
- To maintain the numeric order, it is important to include the zero for numbers 0-9; this will help to retrieve the latest record number.
- Always state dates 'back to front', and use four digit years, two digit months and two digit days: YYYY-MM-DD or YYYY-MM or YYYY or YYYY-YYYY. Giving the dates back to front means that the chronological order of the records is maintained when the file names are listed in the file directory.
- When a file name includes a personal name, give the family name first followed by the initials, or forename.
- File names of records relating to recurring events should include the date and a description of the event.
- The file names of correspondence should include the name of the correspondent, an indication of the subject (if applicable), the date of the correspondence and whether it is incoming or outgoing correspondence.
- The version number of a record should be indicated in its file name by the inclusion of 'v' followed by the version number and, where applicable, 'Draft'. A new version should be created for any changes to the document, other than minor corrections such as typographical errors or spelling mistakes.
- Non-alphanumeric characters in file names should be avoided (as this can cause errors when using certain MS office products).

### **Tracking and Tracing**

- Tracking and tracing procedures should be in place for paper records that enable the movement and location of records to be controlled and provide an auditable trail of record transactions.
- It should be simple and only used with records when the file is moved outside the department.
- The item should be referenced and the file name noted with the person, their position or operational area having possession of the item and the date moved. Remember, that this only applies for Corporate Records and that Patient Records should be moved according to the Trust's Patient Document Tracker as part of the PAS.

### **Protective Markings**

- All records regardless of media may be classified to reflect their status. They should be appropriately marked into different categories such as:
- NHS Confidential
- NHS Protect – this is similar to using the term "Commercial in Confidence" which can be applied to sensitive information that needs to be protected (eg commercially sensitive or personal)

### **Retention and Disposal**

- Records should follow the NHS retention guidance.
- It is a fundamental requirement that all of the Trusts' records are retained for a minimum period of time 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 Trust's business functions.
- A retention, storage and disposal schedule is a timetable for a planned review of all records to determine how long they should be kept for, which is either:

- Permanent retention for records having long term value for the organisation or nationally, or
- Secure destruction of records which the organisation is not obliged to keep for legislative or business reasons.

## Chapter 20: Working from Home

As staff are increasingly working from home, it is essential that basic IG advice, as given throughout this *Handbook* is followed. Further specific guidance is as follows:

### a. Laptop Security

- If you have a work laptop make a note of the laptops asset number to make sure that you have it in the eventuality it gets stolen.
- Ensure that all laptops, records and anything that is valuable to the organisation is kept secure whilst in transit. For example, do not stop at the shops on the way home.
- Turn the laptop off when it is not in use.
- Lock the laptop screen when it is left unattended.
- Ensure there are limited opportunities for the laptop to get broken (e.g. spilt drink).



### b. Physical Records

- If you need paper records these will need to be kept secure, and taken home only with managerial agreement.
- If you create any confidential waste this needs to be securely destroyed. This must not go into general waste. If possible destroy with a cross cut shredder as a minimum. If this is not possible, keep securely until such time as you can bring back to the office and securely destroy there.

### c. Printing

- Printing of confidential data when working from home is not permitted, as devices are not connectable to printers in the home.

### d. Information Security

- If communicating with non-NHSmial users, put [secure] in the subject line ensuring you include the square brackets.
- Report any loss of information, data or equipment immediately.

### e. Post

- Wherever possible send the communication by email instead, using your NHS mail account. Never use a personal email account.
- Avoid getting personal information posted to your house.



## f. Communications

- Ensure you have your work mobile switched on, if you have one. If you do not have a work mobile and need to contact patients ensure you add 141 before every number dialled so that they do not obtain your personal number.
- If you require the use of Video Conferencing the current system of choice for internal meetings is MS Teams. For consultations with patients it is NHS Consult (Attend Anywhere). (See Chapter 17.)

## g. Systems

- If you need access to systems make sure that you can still access them from home.

## h. Environment

- Ensure you consider carefully where you will be working in your home.
- Make sure you have considered the security of that location e.g. lockable windows / doors / cupboards.
- Ensure if you are working with sensitive information you distance yourself from others in the home. Remember that no one else should see your work information.
- Be aware of Smart devices in the home, such as Siri, Alexa and Google Assistant, as there is the possibility that may pick up and record confidential conversations being had on the phone and/or by video conference, and so breach confidentiality. Whilst having such conversations they should be muted or shut off.

## Chapter 21: Storage of Locally-Held HR Records

Management of locally-held staff management records, including their storage, use, transfer or destruction is the responsibility of line managers. This section has been written in association with HR to offer guidance on best practice in managing locally-held records.

Any major records, such as sanctions relating to performance and /

or conduct, or letters of concerns relating to attendance, must be held on the master personal file in HR. Such major records held by managers should only be copies of those major records or minor records should only need to be held for two years, after which they should be securely disposed of. Managers are encouraged to have a “bring forward” system in place in this regard.



- Any hard copy staff records must be held in individual files in a locked drawer away from public areas.
- Managers are encouraged to keep electronic-only records wherever possible and scan existing hard copy records to the e-file, confidentially disposing of the hard copy records once they have been safely scanned in.
- Electronic records must be kept in the secure local drive, in a password-protected folder and not in individual “documents” folders. Password access must only be given to those who need to access staff records and must not be shared more widely. The password should be changed regularly.
- When a staff member transfers to different area, whether on temporary redeployment/secondment or permanently, then any records relevant to their ongoing line management must be securely transferred to the new line manager, with a handover if appropriate. Secure transfer is either by hand, courier delivery or via NHSmail email with confirmation of safe receipt. Any outstanding matters that need to be recorded on an e-roster or ESR should be uploaded / sent to HR Services as appropriate prior to transfer.
- Sickness absence dates are held on ESR so managers are not required to record these locally.
- Occupational Health memos are copied to HR so are not required to be retained locally after the staff member leaves.
- On leaving the Trust, staff management records should be kept for six years from the date of leaving (or the staff member’s 75<sup>th</sup> birthday, whichever is sooner). Managers may wish to keep a separate secure archive e-file to transfer these records into. Only records which are not kept on ESR or by Occupational Health, such as referrals and advice letters/reports, need to be retained.
- With regard to recruitment, once an offer of work has been made to an individual, records from the full selection process, for all candidates, successful and unsuccessful, need to be returned to the Recruitment Team to ensure that they are retained alongside the application details for the required time period.
- If you have any queries on a particular case then you should contact either the IG Team or HR for guidance.

## Chapter 22: Freedom of Information Requests

The **Freedom of Information Act 2000** (FOI) gives members of the public access to **any** recorded information held by public authorities, including the NHS. It promotes transparency and allows the public to hold public bodies to account, both on how money is being spent and how decisions are made which may affect their lives. Access is given in two ways:

- Anyone worldwide is entitled to request any information held by the Trust.
- Certain information about the Trust’s activities is published as part of a Publication Scheme on our public website.

The FOI presumes that information should be disclosed unless there is a good reason not to. Requests can be from members of the public, the media, universities, other NHS organisations, local authorities, charities, MPs, legal professionals, private companies, etc.

Since all of our work-related correspondence is recorded and can be requested via the FOI, it is important to ensure all communication, including emails, remains appropriate and professional.

As a public authority we are required under the FOI to:

- Reply to any request within 20 working days, either by providing the information or stating why it cannot be provided and applying any of the 23 exemptions.
- Provide advice and assistance to applicants making requests.

The Trusts' Publication Schemes can be accessed on the public websites and include the following types of information:

- Who we are and what we do
- What we spend and how we spend it
- Our priorities and how we are doing
- How we make decisions
- Our policies and procedures
- Lists and registers
- The services we offer

All staff have a responsibility to assist with FOI requests when asked to do so. If you receive any requests for information that fall outside of 'ordinary business', they should be referred to the FOI Office using the details given in Appendix 1 as soon as possible.

All staff must include the following information in their Out of Office messages:

*If your email is a request for information made under the terms of the Freedom of Information Act, please send your email to the Trust's Freedom of Information team who will be happy to process your request – [add in FOI email address for respective Trust from Appendix 1]*

Further information about FOI can be found on the **Intranet** or by contacting the FOI Team using the details in Appendix 1.

## Chapter 23: Data Protection Impact Assessments



It is the responsibility of all staff to incorporate IG into their working practices and to also make partner organisations provide assurance that information will be handled in a secure and appropriate manner. As part of the IG framework, responsible managers and staff must consider IG implications when starting new or updating existing projects. It is essential to include the IG Team at the earliest possible opportunity to advise of the

IG elements which will need to be considered.

A DPIA is a risk assessment tool mandated by the **GDPR** that helps to demonstrate an approach that includes 'Data Protection by Design' from the start of a project, proposal, programme or project.

Identifying IG elements at an early stage will help ensure:

- The aims of the project are met wherever possible.
- Compliant operations.
- Necessary information sharing protocols are in place.
- IG and Data Protection risks are minimised.

It will also eliminate the potential of failing to comply with the **GDPR** and subsequent fines from the ICO.

The IT Business Change Team within the Trust also mitigates IG risks as part of their process mapping and testing of systems through the early identification of risks related to PCD and in the assessment of the workflow; this includes ensuring that data is validated during data entry to check accuracy to meet Data Quality standards.

These are logged in an Issues and Risks log and then mitigated as part of the design process. Further checks are undertaken as part of testing to ensure the risk has been resolved.

Clients are also advised regarding PBAC to systems, to ensure users are allocated the correct privileges to view PCD. This is achieved by utilising a security matrix.

The IG Team does its utmost to complete the first review of any DPIAs received by them within two weeks of their receipt.

## Chapter 24: Business Continuity



Business Continuity Management is a process used to identify key services which, if interrupted for any reason, would have the greatest impact upon the community, the health economy and the organisation, to identify and reduce the risks and threats to the continuation of these key services and to develop plans which enable the organisation to recover and / or maintain core services in the shortest possible time.

The fundamental element of business continuity is to ensure that whatever impacts the Trust, the organisation continues to operate. Business Continuity Plans (BCP) will help shape organisational resilience to 'threats', plan counteractions and minimise interruptions to the Trust activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications).

A BCP is the documented collection of procedures and information that is developed and maintained in readiness for use in an incident to enable the organisation or department to continue to deliver its critical activities at an acceptable predefined level.

The Trust's Business Continuity documentation is available on the **Intranet**.

## Chapter 25: Information Sharing

Who can you share information with, and what information can you share? These are not simple questions to answer, but the **GDPR** and IG are not barriers to appropriate sharing. In 2013, for example, a new Caldicott principle was added which promoted that **'The duty to share information can be as important as the duty to protect patient confidentiality'**. This is the guiding principle when considering the sharing of patient information.



It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The Trusts must ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

*Guidance on Information Sharing for Safeguarding Practitioners* updated by the Department for Education in July 2018 has **Seven Golden Rules** of Information Sharing which are broadly applicable to all instances of sharing PCD:

1. Remember that the **GDPR**, **DPA18** and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.



2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your IG lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the **GDPR** and **DPA18** you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Staff sharing personal information with other agencies must be aware of the Trusts' requirement to have an ISA in place for the routine sharing of PCD.

The Trusts work to a three stage process, which has been agreed with other local health and social care organisations in Sussex:

1. **A High level Charter and Principle.** The Trusts achieve this by being signatory to the Sussex-Wide Information Sharing Protocol, adherence to all DSPT Assertions or equivalent assurance, such as certification to ISO 27001, the International Standard for Information Security.
2. **A Risk Assessment.** The Trust realises this with the use of DPIAs to demonstrate the appropriateness of the sharing, that there is a defined legal purpose and security of transfer.
3. **A Local Information Sharing Agreement.** This gives team-level detail regarding how the information will be transferred, by what means and to whom. A template is available from the IG Team and on the **Intranet**.

For further advice and guidance on ISAs, contact the IG Team. The Trusts are increasingly using a system called the Information Sharing Gateway for ISAs to be put in place electronically between organisations.

## Chapter 26: Next of Kin

It is important to be aware that the Next of Kin concept is not formally defined in UK law. A patient's selecting a Next of Kin is not the same as appointing a Lasting Power of Attorney for Health and Welfare, as this role allows them to make health and care decisions for patients if they lose mental capacity. Anyone nominated a Next of Kin by a patient must be an adult of 18 or over.

From a clinical perspective a Next of Kin is someone who is nominated by a patient to receive information about their medical care in an emergency situation. If a patient has not nominated a Next of Kin, it will generally be assumed to be a close blood relative, spouse or civil partner that has been involved with or had an interest in their care.

The Next of Kin will be kept informed about the patient's care whilst they are in hospital.

Being a Next of Kin does not automatically entitle that person to have access to the patient's clinical information of Medical Record.

## Chapter 27: Research



Health research benefits everyone whether they are perfectly well, or have been ill for a long time. It helps find out what causes ill health and supports development of new medicines and healthcare, which can be used right from the start of an illness. Research also helps the Health Service improve delivery so that everyone gets the care they need in the best possible way. Health data is one of the most valuable assets we have. In research, it is brought together from all the different places it is kept and linked to provide

the best possible picture of health and what might affect it. Researchers may use health data in different forms for example:

- **Identifiable data.** This includes names, addresses and dates of birth. This data is used to find people to take part in trials, or answer extra questions about their health history. For example, it might be used to see if where someone lives increases their chances of getting a particular disease or to find out more about a specific treatment.
- **Anonymised data.** This is information that cannot be traced back to a person's Medical Record, making it impossible to identify that person. This data is used when researchers do not need to have any direct contact with you. Sometimes, data is coded so that it can be linked back to an actual person if extra information is needed. This is called pseudonymisation, and is a very helpful part of research that is strictly controlled.

Data Protection legislation is in place to make sure that patient data cannot be abused. Researchers face disciplinary action, or even prosecution, if they do not use data responsibly. An NHS ethics committee, made up of members of the public and professionals, assesses the risks and benefits of individual research studies before they can go ahead. When people can be recognised by their data, only specific people can see the information and it must be stored in a secure place. How this is managed forms part of the overall assessment and approval of research in the NHS.

Obtaining consent to take part in research and for disclosure of any confidential information is an important part of all research trials. The introduction of **GDPR** does not generally mean that researchers have to re-consent participants who are already involved in a research trial.

The screening of Medical Records by care teams for study recruitment is permitted under **GDPR**. NHS organisations need to inform patients through transparency information and uphold confidentiality requirements. Transparency is about better informing patients, public and participants about research so making information understandable and drawing people's attention to it is key.

Researchers can share data with other researchers in line with confidentiality requirements. They will need to anonymise data, or get participants' permission to disclose confidential information to other researchers if participants would not reasonably expect it or if sharing is for a new purpose, i.e. not part of their normal care or if not what participants originally consented to share.

Researchers must also outline what withdrawal from the research project means, particularly with respect to data that has already been collected. Research is largely exempt from the right to erasure, all data about a participant collected as part of research doesn't necessarily have to be deleted. The **GDPR** says any personal data can be used for research, regardless of the initial reason for collection, subject to safeguards, transparency and fairness.

If you have any questions about NHS clinical research and data protection for participants please contact the Research Department or look at the [Health Research Authority website](#).

## Chapter 28: Use of Information for Non-Care Purposes

Information that is to be used or shared for non-care purposes, for the benefit of the community, should generally be anonymised. This is defined by the ICO as the process of turning the data into a form which does not identify individuals and where identification is not likely to take place. This may include research, commissioning and assessing the quality and efficiency of services. If the purposes can be achieved with anonymised information then they must be. This means that the information will have all identifiable information that may identify an individual permanently removed from it.



Direct identifiers that need to be removed for anonymisation are:

- Name
- Date of birth
- Address
- Postcode
- NHS number
- Hospital number
- Telephone number
- Email Address
- Any other widely-used unique person or record identifier (e.g. spell or episode or attendance number)

Pseudonymisation within a trusted and safe environment may be an acceptable alternative. This is similar to anonymisation, and is defined by the ICO as the process of giving individuals in a dataset a unique identifier which does not reveal their real identity. Whereas this is still defined as personal data under Data Protection legislation, its use can help reduce privacy risks by making it more difficult to identify individuals. In other words pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information (the 'key'), provided that such additional information is kept separately and is subject to technical and organisational measures such as password protection and/or encryption.

One of the pseudonymisation techniques is the practice of extracting and replacing actual identifiers with a coded reference (the 'key'), where there is a means of using that key to re-identify an individual. This approach is typically used where the use of the data needs to relate to individual records, but also needs to retain security and privacy for that individual.

Pseudonymised data carries a higher privacy risk and security of the key is essential. Because the data is not truly anonymised, personal data that has been pseudonymised can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym (the 'key') to a particular individual.

Identification is achieved in one of two basic ways:

- Direct identification, where only a single data source is necessary to identify an individual.
- Indirect identification, where two or more data sources are needed to be combined to allow an individual to be identified.

The difficulty in determining whether the anonymised data you hold or wish to share is personal data lies with not knowing what other information is available to a third party that might allow re-identification to take place. This requires a case-by-case judgement of the data.

If the need to use the information cannot be achieved by either anonymisation or pseudonymisation, then patient consent is generally required. The only exemption to this is if there is an overriding and statutory basis for breaching confidentiality, including:

- Compliance with a Court Order
- Notifiable Diseases to Public Health England
- To support the prevention or detection of serious crime
- Under s251 of the **National Health Service Act 2006** when ordered by the Secretary of State for Health and Social Care
- NHS Digital has powers to request information which are binding on health bodies, although such powers may not be enforced where a patient has objected

These are complex issues which will typically require expert advice and consideration. Staff faced with decisions on such matters should have regard to national guidance and seek advice from the IG Team. Key guidance includes:

- DH's [Confidentiality NHS Code of Practice](#) (Annexe C).
- NHS Digital's [Guide to Confidentiality in Health and Social Care](#).
- ICO's [Anonymisation: Managing Data Protection Risk Code of Practice](#).
- NHS Digital's [Anonymisation Standard for Publishing Health and Social Care Data](#).

## Chapter 29: The National Data Opt-Out



Patients are entitled to opt-out of their confidential information being used for research or planning purposes. The national data opt-out does not apply to information that is anonymised in line with the ICO's [Anonymisation: Managing Data Protection Risk Code of Practice](#) or is aggregate or count type data.

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian, Dame Fiona Caldicott, in her *Review of Data Security, Consent and Opt-Outs*.

Patients can view or change their national data opt-out choice at any time by using the online service at [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters) or by calling 0300 3035678.

By 31 March 2021 all health and care organisations are required to be compliant with the national data opt-out policy. NHS Digital and Public Health England are already compliant and are applying national data opt-outs.

To query the national data opt-out status of a patient(s), or for any other queries regarding the national data opt-out service:

- For BSUH contact [REDACTED]
- For WSHFT contact [REDACTED]

## Chapter 30: Smartcards

Smartcards are required to use and access IT systems essential to healthcare provision. Primary Care Contractors need to use Smartcards in order to gain access to patient information, including those who provide the NHS e-Referral Service and the Electronic Prescription Service.

Individuals are granted access to a Smartcard by the organisation's Registration Authority (RA) Team. It is up to the Trust's RA Team to verify the identity of all healthcare staff that need to have access to PCD. Individuals are granted access based on their role and their level of involvement in patient care.

**All staff issued with a Smartcard and passcode must be aware that they must comply with the terms and conditions of issue. Failure to do so will be dealt with as a serious disciplinary matter. Staff must not share or allow usage of their Smartcards by colleagues, including managers, peers or IT personnel, for any reason.**



The use of Smartcards leaves an audit trail detailing access and usage, including only having viewed a record. **This audit information may be used in disciplinary procedures regarding inappropriate or unauthorised access to systems.**

### **a. Line Manager Responsibilities**

- To identify all roles within their area of responsibility which require access to the system and ensure that staff, including employees, bank, locum, agency workers, contractors, volunteers and office holders, are provided with appropriate access.
- To ensure for all roles that involve access to the system that job descriptions and any recruitment materials make reference to the need to be registered and the role's responsibilities in relation to using the system.
- To ensure that all new starters within their area of responsibility, including agency / temporary employees, receive training in order to be able to access the system.
- To ensure that all staff are aware of the IG & RA policies and their responsibilities in relation to use of and access to the system.
- To ensure that access to systems is appropriately amended when staff change job roles to avoid excessive access.
- To ensure the Trust's leavers' policy is followed when a member of staff leaves the organisation.

### **b. Staff Smartcard Code of Practice**

- Use your Smartcard responsibly and in line with your access rights.
- Report on Datix the loss, theft or misuse of your Smartcard.
- Replacement cards can be obtained:
  - At WSHFT via the IT Self Service icon or emailing [REDACTED]
  - At BSUH by emailing the RA Team on [REDACTED]



- Ensure that you keep your Smartcard and log-in details confidential. In particular you must not leave your PC logged in and you must not share or provide access to your Smartcards or passwords.
- All members of staff using Smartcards must follow the Trust's IG & RA policies and procedures, and adhere to the Data Protection and Caldicott Principles.

## Chapter 31: Data Quality



Data Quality is vital to the decision-making processes of any organisation. This is particularly important for a public service such as the NHS where financial integrity and public responsibilities of care need to be ingrained in the services provided. Understanding of what Data Quality actually is can vary dramatically so to address this the Trusts have a framework for Data Quality evaluation which can also be used as an introductory guide to Data Quality.

While Data Quality is neither a business issue nor a technical issue it should be used to enhance both. It is important to stress that **Data Quality is everyone's responsibility**.

Data Quality can be defined as captured information that is consistently fit for its intended use in representing real world figures and situations to help inform operational decision making and planning, risk assessment and financial transactions.

Understandably then, the IG Team frequently receive enquiries about how to change information on PAS, such as names, addresses, DoB, hospital numbers, GPs, referrals and the existence of duplicate records.

Whereas the quality and integrity of data is broadly an IG issue, it is managed at BSUH by the **Corporate Data Team** and at WSHFT by the **Data Quality Team**.

Their aim is for the Trusts to hold the most accurate and up-to-date information on our patients and to make sure that the activity against them is recorded correctly. They understand that anomalies and circumstances can sometimes present difficulties for PAS users so are keen for you to call them if you need help.

BSUH has developed two eLearning courses available on IRIS to help as part of staff training on Data Quality. The **Data Quality Awareness** module is available [REDACTED] After completing this course delegates will have a greater understanding of Data Quality and be confident in dealing with issues when they arise. On completing the **Patient Identification** module [REDACTED] delegates will learn some of the reasons why duplicate patient records might occur, consequences of this and learn strategies to improve overall record keeping.

For queries regarding BSUH Corporate Data Team or WSHFT Data Quality, please use the contact details in Appendix 1.

## Chapter 32: When Staff Become Patients

We nearly all have times in our lives when we are poorly or have had an accident. Confidentiality concerns can, however, naturally arise when staff find themselves becoming a patient.



It is appreciated that this situation can cause a blurring of staff / patient boundaries but it is important that staff respect the potential for confidentiality breaches as with any other patient / professional relationship.

If, as a member of staff, you have a hospital appointment or you become an inpatient, you become a patient for the duration of your appointment / treatment, including any time spent in the waiting area.

It is understood that staff do not wish to 'waste time' waiting for appointments when they could be working and that their absence from their department impacts on their colleagues. This commitment to work is admirable, however, to avoid confidentiality issues, the Trusts' advice is to remove yourself from your professional role and attend your appointment as you would if you were a patient who is a member of the public.

If you see a member of staff waiting for an appointment or as an inpatient, please respect their confidentiality and don't ask them, or another member of staff, why they are there. Neither should their Medical Records or any electronic information, such as the PAS system, about them be looked at unless there is a legitimate reason to do so as part of the team treating them or administering their information as a patient. Wanting to know their location as an inpatient is not a legitimate reason, even if it is out of genuine concern. Neither must staff involved in the patient's care discuss with another staff member any aspect of the patient's condition / care unless they are directly involved in their care.

Staff requesting updates to their own waiting list or admission status should approach a member of the Admissions or Waiting List staff rather than their health care professional.

An example of confidentiality being breached is a member of staff attending an appointment and, as the clinician is running late, asking the Receptionists if they would make contact when the Consultant is ready, either by phoning their internal extension or advising them in person. This could result in messages containing appointment details being left on a work voicemail and being played back in an open office, or being taken off the phone by a colleague. Advising in person at their place of work could involve language being used that alerts colleagues to the nature of their appointment, or that they have an appointment at all.

**When staff become patients they *are* patients, and the same dignity must be given to them and their personal information as with all other patients.**

## Chapter 33: Management of Third-Party Contracts

A checklist must be used to sign-off formal written third-party contracts where third-parties, i.e. Data Processors, will have an interaction with patients or staff and / or their PCD, so as to demonstrate that it has appropriate IG clauses included. If, however, the NHS Standard Contract or NHS Terms and Conditions of Contract are used, it is not necessary to complete this checklist, as it incorporates appropriate IG assurance clauses.

**It is the joint responsibility of the Commissioning / Procurement Team**



**and the owning Manager of the contract to ensure this Checklist is completed and held locally.**

All of the following requirements must be met; otherwise a third-party contract is invalid from an IG perspective.

- **Data Protection and Cyber / Information Security:**

- The Data Processor may only engage another processor with specific written authorisation of the Data Controller.
- The Data Processor ensures that if they engage another Data Processor for carrying out specific processing activities on behalf of the Data Controller, they ensure the same Data Protection obligations are imposed on them.
- The following are defined:
  - Subject-matter and duration of the processing.
  - Nature and purpose of the processing.
  - Type of Personal Data.
  - Categories of Data Subjects.
  - Location of primary data hosting and backup arrangements.
  - Obligations and rights of the Data Controller.
- The Data Processor will only process Personal Data on documented instructions from the Data Controller.
- The Data Processor will only transfer Personal Data to a third country or international organisation where there are appropriate safeguards and only if Data Subject rights are legally enforceable there; typically, this means an approved third country with an adequacy decision by a Supervisory Authority, Binding Corporate Rules, or the use of model contract clauses.
- The Data Processor ensures the confidentiality of the data being processed.
- The Data Processor ensures the technical and organisation security of the data being processed (i.e. Information Security of both paper and digital records), by use of, for example, encryption and pseudonymisation, as well as contractually-agreed backup, restore and recovery processes.
- The Data Processor responds to and / or appropriately supports Subject Access Requests within a predefined timescale, so as to allow the Data Controller to respond to the requestor within the month timescale.
- The Data Processor will appropriately inform the Data Controller of any Data Breaches (including IG, Information Security, Cyber Security and other related breaches) at the earliest opportunity and no later than 24 hours from becoming aware of the data breach to enable the Data Controller to meet its 72 hours reporting obligation.
- The Data Processor ensures will cooperate with the Data Controller in informing Data Subjects if their data has been breached.
- The Data Processor ensures will cooperate with any third party incident responders appointed by the Data Controller, national CareCERTs (if health and social care bodies) and law enforcement agencies through the incident management lifecycle.
- The Data Processor ensures will fully engage with both Privacy by Design, including DPIA, processes when developing new and / or significantly updating existing information systems (paper or digital).
- The Data Processor will return all Personal Data to the Data Controller at the end of the provision of services and only delete any copies upon instruction by the Data Controller (having first confirmed that data integrity has been maintained in the transfer or that the data are not required as per retention schedule).
- The Data Processor will allow the Data Controller's preferred penetration testing organisation to actively scan infrastructure hosting digital information for vulnerabilities and to exploit these for the purposes of evidence to the Data Controller and Data Processor.

- **Freedom of Information**

- Duty to disclose (or to support disclosure if a non-public body).
- Any exemptions to disclosure provisions.
- Responsibility for FOI applications.

- **General**

- Penalties for breach of IG clauses are detailed.
- Provisions to indemnify the Trust against breaches by the third party are outlined.
- Responsibilities for costs, e.g. for Information Security audit, Subject Access Requests and FOI etc.
- The Data Processor will allow Data Protection and related compliance audits of the service provided (without notice where possible or at 24 hours' notice).

## Chapter 34: Counter Fraud

Fraud within the NHS is an unfortunate reality, committed by patients, staff and external parties alike. It is important that funds which are intended for healthcare are used as such; therefore the Trust takes a zero tolerance approach and is committed to tackling any instances of fraud by means of applying appropriate sanctions, including criminal action.

For an offence of fraud to be committed, the offender must have acted dishonestly with the intent to make a gain for themselves or another, or cause a loss, or expose another to the risk of a loss (i.e. the NHS). The three main offences under the **Fraud Act 2006** are:

- False representation.
- Failure to disclose.
- Abuse of position.

### **a. Identity fraud**

Identity fraud is a common fraud type within the NHS and can occur as a direct result of poor IG. If enough personal information is available, criminals can use it for monetary gain. This can enable job applicants to use falsified documentation, such as a fake passport or driving licence, for the purposes of obtaining employment, or free healthcare for non-UK residents.

Identity fraud can happen in a number of ways in the NHS but the most concerning is when a person purports to be a clinician. A bogus doctor was able to gain employment in an NHS Trust having created fictitious paperwork. He was eventually caught and jailed but this highlights the importance of keeping personal data safe and undertaking diligent checks to ensure qualifications are held and genuine.

### **b. Current email scams**

Email scams, also called phishing scams, are becoming increasingly common as fraudsters come up with new ways to try and trick you into clicking on a link or stealing personal information. We have listed below the current scams that you should be aware of.

Remember, if you are in any doubt about the origin of an email, do not open it.

### **c. NHSmail and email phishing frauds**

Several NHSmail users have reported receiving an email with the subject 'suspicious url: urgent.' The email suggests that it is an NHS email update programme and the user must click on the link to update their email account. Do not click on the link and delete the email both from your inbox and deleted items folders.

Emails are being sent to NHS email accounts purporting to be from genuine agencies such as the HMRC and DVLA the email contains a link to the website. Spare a moment to think why you would get an email from this agency and verify the sender is genuine by visiting the website from the search menu. Do not click on the link and delete the email both from your inbox and deleted items folders.

### **d. CEO email phishing frauds**

CEO frauds are when the fraudster pretends to be the CEO and request for an urgent payment to be made. The fraudster will provide bank details and use information about the organisation (such as a reference to another senior member of staff by name) to try and authenticate their request. Do not make any payments and always make personal contact with the person sending the request to validate.

### **e. Reporting concerns**

If you have suspicions that fraud may be occurring or wish to receive further information about any of the above, please contact your Local Counter Fraud Specialist using the contact details in Appendix 1.

Alternatively, you can report any concerns to the NHSCFA on 0800 028 40 60 (between 8am and 5pm, Monday to Friday) or via the online reporting form [www.cfa.nhs.uk/reportfraud](http://www.cfa.nhs.uk/reportfraud). All information provided via this secure website is completely confidential.

It is the LCFS' role to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern. It is recommended that you refer to your organisation's policy on fraud when reporting allegations for further information on how you are protected.



## Appendix 1 – Contact Details



Brighton and Sussex  
University Hospitals  
NHS Trust

[REDACTED]

[REDACTED] – Group Director of IM&T / SIRO

### Confidential Waste Team

### Corporate Data Team

[REDACTED] – IG Manager

### Freedom of Information Team

[REDACTED] Operational IG Lead

[REDACTED] – Group FOI Manager

[REDACTED] Medical Director / Caldicott Guardian

[REDACTED] – Group Head of IG / DPO (Strategic IG Lead)

### Local Counter Fraud Specialist

[REDACTED] IG Manager

### Subject Access Request Team

[REDACTED] – IG Manager



Western Sussex Hospitals  
NHS Foundation Trust

[REDACTED]

[REDACTED] – Group Director of IM&T / SIRO

**Confidential Waste**

[REDACTED]  
[REDACTED]

**Data Quality Team**

[REDACTED]  
[REDACTED]

**Freedom of Information Team**

[REDACTED]

[REDACTED] Group FOI Manager

[REDACTED]  
[REDACTED]

[REDACTED] Group Head of IG / DPO

[REDACTED]  
[REDACTED]

[REDACTED] IG Manager

[REDACTED]  
[REDACTED]

[REDACTED] Consultant Paediatrician / Caldicott  
Guardian

[REDACTED]

**Local Counter Fraud Specialist**

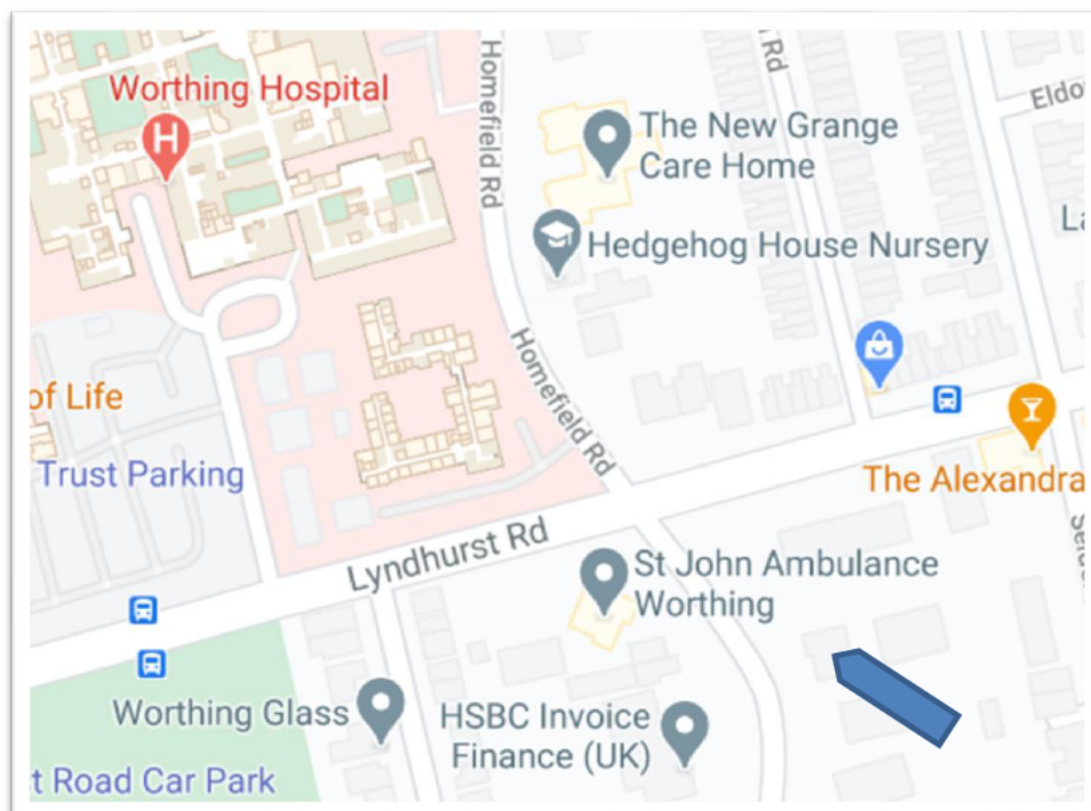
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] – IG Manager

[REDACTED]  
[REDACTED]

**Subject Access Request Team**

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



## Appendix 2 – Staff Employment Records Privacy Notice

During the course of its employment activities, the Trust collects, stores and processes personal information about prospective, current and former staff.

This Privacy Notice includes applicants, employees (and former employees), workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat the personal and sensitive data of staff in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met.

### What types of personal data do we handle?

In order to carry out our activities and obligations as an employer we handle data in relation to:

- Personal demographics (including, but not limited to, gender, race, ethnicity, sexual orientation, religion, age, marital status, disability, gender reassignment)
- Contact details such as names, addresses, telephone numbers and emergency contact(s)
- Employment records (including professional membership, references, proof of eligibility to work in the UK and security checks)
- Management records (including, but not limited to, documentation relating to appraisal, training, attendance, conduct and performance management, organisational change processes and payroll data)
- Bank details
- Pension details
- Medical information including physical health or mental condition (for example occupational health information)
- Information relating to health and safety
- Trade union membership
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment Tribunal applications, complaints, accidents, and incident details
- Referrals to regulatory bodies e.g.: GMC/NMC/HCPC

Our staff are trained to handle your information correctly and protect your confidentiality and privacy. We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your information is never collected or sold for direct marketing purposes. Your information may be processed overseas. During the recruitment episode references and police checks may be requested from overseas if this is required to satisfy the necessary checking processes.

### What is the purpose of processing data?

- Staff administration and management (including payroll and performance)
- Pensions administration
- Business management and planning
- Accounting and Auditing
- Accounts and records
- Crime prevention and prosecution of offenders
- Education
- Health administration and services
- Information and databank administration
- Sharing and matching of personal information for national fraud initiative

We have a legal basis to process this as part of your contract of employment (either permanent or temporary) or as part of our recruitment processes following data protection and employment legislation.

## **Retention Periods**

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Retention periods for personal data will vary according to the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

You should be aware that employee documentation is ordinarily retained for six years after termination of employment, which is the statutory limitation period for breach of contract claims, and then promptly deleted once that period has passed. For unsuccessful job candidates, documentation is retained for twelve months after the candidate is rejected for a role and then deleted.

If we are able to anonymise your personal data so that you can no longer be identified from it, we may use such information without further notice to you.

## **Sharing your information**

There are a number of reasons why we share information. This can be due to:

- Our obligations to comply with legislation
- Our duty to comply any Court Orders which may be imposed

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

## **Use of Third Party Companies**

To enable effective staff administration the Trusts may share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer.

We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation.

## **Individuals Rights**

Data Protection law gives individuals rights in respect of the personal information that we hold about you. These are:

1. To be informed why, where and how we use your information.
2. To ask for access to your information.
3. To ask for your information to be corrected if it is inaccurate or incomplete.
4. To ask for your information to be deleted or removed where there is no need for us to continue processing it.

5. To ask us to restrict the use of your information.
6. To ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information.
7. To object to how your information is used.
8. To challenge any decisions made without human intervention (automated decision making)

Please visit our Trust Website for further details. Should you have any further queries on the uses of your information, or your obligations in relation to the new legislation, please speak to the Human Resources Department or our Data Protection Officer on [REDACTED]

Should you wish to lodge a complaint about the use of your information, please contact our Human Resources Department. If you are still unhappy with the outcome of your enquiry you can write to: The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF - Telephone: 01625 545700.



## Consultation, Distribution and Acknowledgements

### a. Internal Consultation

This *Handbook* was electronically signed off as appropriate for distribution to all staff by the Trusts' joint IG Steering Group on 17 September 2020. In addition to members of that group, several others very kindly reviewed sections relevant to their area of work. These include:

- [illegible]

██████████ the Trust's IG Team for their unwavering support throughout the year, and input into this *Handbook*. Without them in particular, it would not be what it is.

### b. Distribution

As part of the same consultation, the IG Steering Group agreed the following distribution process:

- Posting on the **Intranet**.
- Via email to managers, containing a link to the document on the **Intranet**.
- The note within that email to:
  - Ask managers of staff without computer / email access to share it with them.
  - Ask managers to ensure copies are available in all staff areas.
  - Include a reference to the disclaimer on p.4.

The IG Team also maintains a supply of hard copies for distribution upon request.

### c. External Acknowledgements

As Editor of this *Handbook*, I offer grateful thanks to several external IG colleagues who have generously shared documents and advice for previous editions that has greatly helped inform its development over the years. These include, but I'm sure are not limited to [REDACTED]

Over time some have moved from the original organisation they were working for when providing earlier support, nonetheless, their input is still massively appreciated. Without all of these, and many others too numerous to name individually, the document would not be as comprehensive as it is. I thank you all.

Group Head of Information Governance / Data Protection Officer

## Notes

[illegible]

[illegible]



**If you would like the *Information Governance Staff Handbook* in any other format or language, please contact the Information Governance Team, which will do its utmost to facilitate this for you.**

***The Information Governance Team's Mission Statement:***

**Ensuring that the Trusts and their staff have a **person-centred** approach to managing the personal and sensitive information of patients and staff, treating it and the organisations' corporate information in a similar manner to which staff would expect their own Medical Records or banking information to be treated.**

Format and original material © (2020)



**Information Governance Team**