



INFORMATION GOVERNANCE

Staff Handbook 2017-18



Applicable to all employees, including
Bank, Locum, Agency, Contractors,
Volunteers and Non-Executive Directors

Current version: v3.0, September 2017
Next review: July 2018

STAFF CONFIDENTIALITY CODE OF CONDUCT

For employees, including Bank, Locum, Agency, Contractors, Volunteers and Non-Executive Directors

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 Management Framework** and the **Information Governance Staff Handbook**, both of which are available in full on StaffNet. 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 patient, 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 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 correct at time of publication.

The *Confidentiality NHS Code of Practice* is mentioned throughout this *Handbook*. Although still a current document, much has changed with Information Governance best practice, so caution must be exercised and advice sought.

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

Any suitable comments or amendments will be incorporated at the next review, due to be published in autumn 2018.

Contents

	New! Staff Confidentiality Code of Conduct	2
	Preface	6
	Acronyms	7
	Introduction	8
Chapter 1	The Trust's Information Governance Personnel	9
Chapter 2	Legislation, Regulations, Guidance and Trust Policies	9
Chapter 3	Caldicott Principles and Data Protection Law	11
Chapter 4	Guide to Confidentiality	12
Chapter 5	Parental Responsibility	19
Chapter 6	Subject Access Requests	21
Chapter 7	New! Sharing Information with the Police	22
Chapter 8	Information Governance and Cyber Security Breaches	23
Chapter 9	New! Management of Clinician to Clinician Handover Sheets	24
Chapter 10	New! Decommissioning Work Areas: Checking for Confidential Information	25
Chapter 11	Monitoring Access to Personal Confidential Data	26
Chapter 12	Information and Cyber Security	26
Chapter 13	Use of Email	29
Chapter 14	New! Patients and the Public Taking Photographs	31
Chapter 15	Information Governance Mandatory Training	32
Chapter 16	Records Management	32
Chapter 17	Freedom of Information Requests	34
Chapter 18	Data Protection Impact Assessments for New and Existing Projects	34
Chapter 19	Business Continuity	35
Chapter 20	Information Sharing	35
Chapter 21	Use of Information for Non-Care Purposes	36
Chapter 22	Smartcards	37
Chapter 23	Data Quality	38
Chapter 24	New! When Staff Become Patients	38
Chapter 25	Counter Fraud	39
Chapter 26	Current Affairs	40
	Consultation, Distribution and Acknowledgements	41

Preface

Dear colleagues

We are delighted to welcome you all to this thoroughly revised and updated Third Edition of the Trust's *Information Governance Staff Handbook*. It complements the annual mandatory Information Governance (IG) Training which all staff are required to attend 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 guidance 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 Second Edition, last year.
- Taken account of the results from the Trust's 2017-18 Confidentiality Audit, as this demonstrates where extra support is needed.
- Updated the News section to cover real incidents and issues over the last year in other NHS organisations to illustrate the real, and often costly, outcomes when IG goes wrong.
- Agreed a distribution plan with the Trust's IG Assurance and Strategy Group so everyone either gets a copy, or knows where it is available to them.

Significant changes in Data Protection legislation are due in May 2018. The IG Team have been working hard behind the scenes to ensure this is implemented smoothly across the Trust for some months. This new law, the EU General Data Protection Regulation (often known as the GDPR), will (despite Brexit and the General Election!) be implemented in the UK and affect all of us in matters of patient and staff confidentiality and privacy. This *Handbook*, and future editions, is key to supporting staff with those changes. Please see p.9 for more details.

Should you need specific IG advice and support, please do not hesitate to contact the team using the details on the back cover 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 on p.9).

Ian Arbuthnot

Director of IM&T

Senior Information Risk Owner

Dr Mike Linney

Consultant Paediatrician

Caldicott Guardian

September 2017

Acronyms

BCP	Business Continuity Plan
DH	Department of Health
DPA	Data Protection Act 1998
DPIA	Data Protection Impact Assessment
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation 2016
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IGT	Information Governance Toolkit
IM&T	Information Management and Technology
ISA	Information Sharing Agreement
PBAC	Person-Based Access Controls
PCD	Personal Confidential Data (see p.8 for full definition)

Introduction

Information Governance (IG) is the practice used by all NHS organisations to ensure that information is efficiently 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 providing 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 (DH) IG Toolkit (IGT) (see p.10), which sets out robust guidelines with regard to IG. Results from the Confidentiality Audit undertaken by the Trust in summer 2017 have also been analysed to ensure the most relevant and up-to-date advice is available to you. The *Handbook* is reviewed annually.

Throughout this document, the term **Personal Confidential Data (PCD)** is used, this is defined as:

Personal information about identifiable individuals, whether alive or deceased, for whom there is a duty to maintain confidentiality. It includes patients, and staff, and incorporates name, address, date of birth, telephone number, NHS number, national insurance number, credit card number, blood group, and weight etc. It also incorporates sensitive data, such as ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health, sexual life, alleged offences and criminal conviction.

IG enables organisations to embed policies and processes to ensure that PCD is processed fairly and lawfully and is:

- H**eld securely and confidentially
- O**btained fairly and efficiently
- R**ecorded accurately and reliably
- U**sed effectively and ethically
- S**hared appropriately and lawfully

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 note.

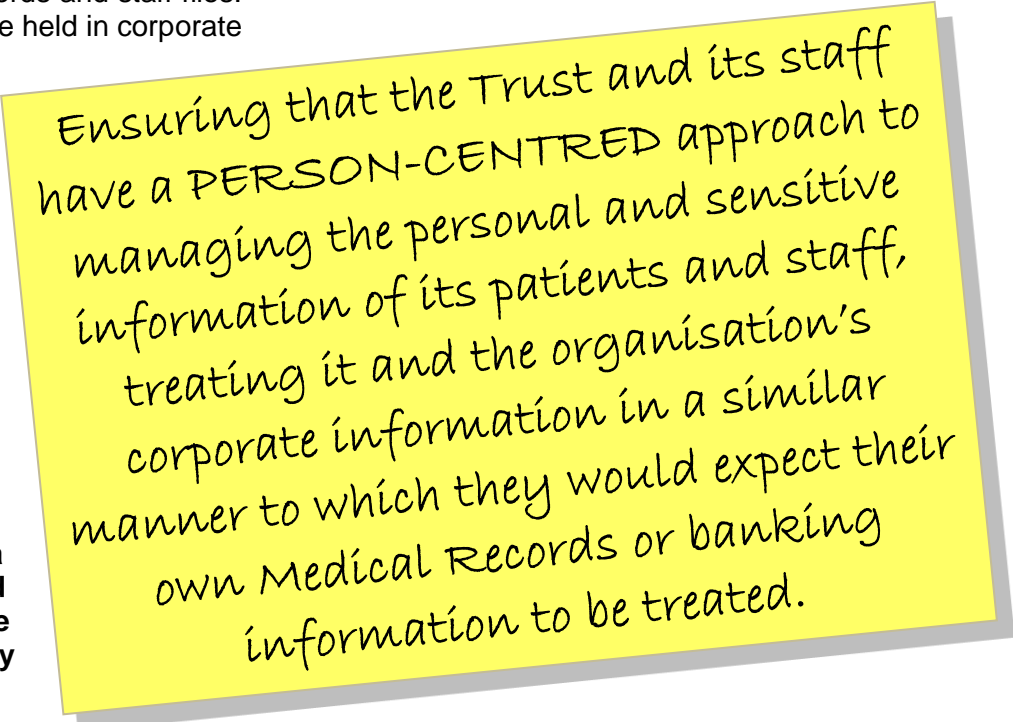
NHS organisations hold vast amounts of PCD, and all staff should be able to provide assurance that the IG standards are incorporated within their working practices. PCD can be contained within a variety of documents, such as Medical Records and staff files.

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

Further details on types of information are available within the [Confidentiality NHS Code of Practice](#) (2003).

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.



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.

Chapter 1: The Trust's Information Governance Personnel

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 **Marianne Griffiths**.

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 risk management across the organisation. The SIRO is supported by the Trust's IG Team. The role is held by **Ian Arbuthnot**, Director of Information Management and Technology (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. The Caldicott Guardian is supported by the Trust's IG Team. The role is held by **Dr Mike Linney**, Consultant Paediatrician.



d. The 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 **IGT** (see p.10). It also supports the Trust in coordinating Serious Incidents Requiring Investigation, offering advice and ensuring the organisation complies with legislation, policies and protocols.

The members of the team are:

- **Jacqui Campbell**, Subject Access and Business Support Manager
- **Andrew Harvey**, Head of Information Governance
- **Tim Hunt**, Information Governance Manager
- **Denise Mahy**, Information Governance Manager

There are also five members of IG staff who process patient Subject Access Requests (SAR) (See Chapter 6).

e. Information Asset Owners

The SIRO is supported by Information Asset Owners (IAO). The role of IAO is to understand what information is held, what is added and what is removed, 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 also be aware of the legislation and guidance surrounding IG that says how 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 1998
- Freedom of Information Act 2000
- General Data Protection Regulation 2016 (from May 2018)
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- *Confidentiality NHS Code of Practice* (2003)
- 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
- *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)

Advice and guidance in the field of Data Protection and IG has historically been produced by NHS England, NHS Digital, DH and the Information Commissioner's Office (ICO), that latter of which is the UK's independent authority set up to regulate Data Protection legislation (see Chapter 3). Increasingly this is being coordinated through the IG Alliance publishing house.

b. Information Governance Toolkit

From all of this legislation, advice and guidance, NHS Digital manages, on behalf of DH, the **IGT**. This is a term that will be used throughout the *Handbook*. The **IGT**:

- Is a self-assessment piece of software mandated for use by NHS, social care, GPs, commercial third parties and other providers of NHS/healthcare-related services to self-audit their IG compliance.
- For Acute trusts has 45 requirements, each of which are broken down to three levels of compliance. NHS Digital mandates that all organisations must obtain at least Level 2 on each of these requirements (which ensures the required score of a Level 2 overall).
- Creates a year-long work programme each financial year, facilitated by the IG Team, to ensure the Trust remains compliant.
- Is subject to both internal and external audit.
- Has reports available online showing the level at which each organisation that has completed it has scored.
- Supports the Trust in bidding for services being commissioned by Clinical Commissioning Groups by demonstrating good IG practice within the organisation.

The **IGT** is due to be replaced with another renamed tool in April 2018.

c. Trust Policies

To support the completion of the work programme, the Trust has a suite of policies, processes and procedures, based on this legislation and guidance including, but not limited to:

- Anti-Virus Policy
- Business Continuity Management Policy
- Confidentiality Audit Procedure
- Consent Policy
- Disclosure of Information to the Police Policy
- Electronic Messaging Policy
- Email Policy
- Email Acceptable Use Policy
- Encryption Policy (*pending*)



- Freedom of Information Policy
- Health Records Policy
- Information Governance Policy and Management Framework
- Information Lifecycle Policy for Corporate Records
- Information Security Policy
- Internet Acceptable Use Policy
- Network Security and Access Control Policy
- Password Policy
- Privacy Impact Assessment Policy
- Remote Access Policy
- Subject Access Request Policy

At time of writing, due to changes in Data Protection legislation and as a result of the May 2017 “WannaCry” ransomware attack that hit the NHS and many other organisations, several of these policies are being re-written. Most recent versions, even if their titles have changed, can be found on **StaffNet**.

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 we hold about them and what we do with it in several ways, including:

- Privacy Notice posters in public waiting areas.
- A Privacy Notice on the Trust external **website**.
- Copies of leaflets that expand upon the Privacy Notice posters which are available in public areas of the Trust, on the **website** and to staff on **StaffNet**.

Chapter 3: Caldicott Principles and Data Protection Law

a. The Caldicott Principles

The Caldicott committee made recommendations in 1997 aimed at improving the way the NHS uses and protects confidential information. Updated in 2013, all NHS staff must be aware of the 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

b. Data Protection Legislation

Until May 2018, when the law will change, all organisations in the UK must comply with the Data Protection Act 1998 (**DPA**), which is enforced in the UK by the ICO, that has the power to fine organisations up to £500,000 for data protection breaches (see examples in Chapter 26). Under Section 55 of the **DPA** it is a criminal offence to unlawfully obtain / disclose personal data or unlawfully sell / offer to sell it on. **If found guilty of committing either of these offences it could result in individuals receiving a personal unlimited fine in Court**, as happened in 2013 to a pharmacist from another Trust that was found to be unlawfully accessing Medical Records of family members, work colleagues and local health professionals. His fine, with costs, totalled over £1,700. **You could also face disciplinary proceedings which may result in dismissal or being struck off a professional register.**



There are eight **DPA** principles that must be followed when handling PCD:

1: Process it fairly and legally
2: Process it for limited purposes and in an appropriate way
3: It must be relevant and sufficient for the purpose
4: It must be accurate
5: It must not be kept for longer than necessary
6: It must be processed in line with the individual's rights
7: It must be kept secure
8: It can only transferred to countries with suitable data protection controls

Full guidance regarding the **DPA** is available on the government's [Legislation Website](#), the [ICO website](#), or from the IG Team.

On 25 May 2018, the EU General Data Protection Regulation (GDPR) becomes active. Despite being an EU regulation, Brexit and the 2017 General Election it will become law in the UK. It will fully replace the **DPA**, and much of it sounds very similar. Where previously there were eight principles for handling PCD under the **DPA**, the **GDPR** has 6:

1: Process it lawfully, fairly and transparently
2: Process it for limited purposes
3: Process the minimum amount needed
4: Ensure its accurate
5: It must be kept for no longer than necessary
6: Keep it secure

However, alongside these, Data Subjects have eight new / expanded rights about their data. These are to be informed how it is used; to have access to it; to have it corrected if wrong; be forgotten; to restrict its use; notification; data portability; objection to processing and to be assured decision made about them are appropriate. The full text is available in the [Official Journal of the European Union](#), with further explanation on the [ICO website](#).

Chapter 4: Guide to Confidentiality

Confidentiality in the NHS is guided by the [Confidentiality NHS Code of Practice](#) (2003). Despite being nearly 15 years old, this is still a current document that sets out required standards of practice concerning confidentiality.

To compliment the national Code, the Trust has a **Confidentiality Code of Conduct**, which is issued to new staff at recruitment, reproduced in the front of this *Handbook* and available for everyone on **StaffNet**.



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.

The **Common Law of Duty of Confidentiality** requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or Court Order requirement to do otherwise.

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 the **DPA**, 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 information held about them, and have errors corrected.
- Individuals, both patients and staff, have the right to request copies of information.
- 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 Clinical Commissioning Groups, under current legislation commissioners can only process or have access to it if:

- **Consent has been obtained from the patient, or**
- **The data has been anonymised (see Chapter 21), or**
- **The data is in respect of safety, safeguarding or the public interest.**

Any decision taken to share PCD as a result of the above must be documented and agreed in discussion with the IG Team, the SIRO and/or Caldicott Guardian. This should then be stored within the 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. Organisational Arrangements

Make sure you know the name of the following:

- **SIRO** – Ian Arbutnot, Director of IM&T
- **Caldicott Guardian** – Dr Mike Linney, Consultant Paediatrician
- **Head of Information Governance** – Andrew Harvey

b. Limiting Unnecessary Access to Personal Information

- Do not discuss confidential matters outside of work, during breaks in public areas, or even 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 still breach a confidence of which you are unaware.
- Do not leave working papers lying around the ward or office, or put confidential items exposed in in-trays.
- Remove documents from photocopiers and fax machines 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 or media 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, typically using the lower case of the keyboard. Some systems require you to use special characters, such as ? and !

- Passwords must not be written down, unless this is in an encrypted format.
- Ensure that computer monitors cannot be seen by other people, especially in public reception areas.
- Lock your computer whenever you are not using it, even for short periods, by using 'Ctrl-Alt-Del'.
- Do not allow **anyone** else to use your log-on to any Trust computer or computer system. To do so breaches the **Computer Misuse Act 1990**.



c. 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. Access to Medical Records is controlled by swipe cards into the department; for electronic systems this is governed by a process called Person Based Access Controls (PBAC).
- 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 control.
- Never send PCD outside the Trust without appropriate level of authorisation or protection.

d. 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 informed consent, are relevant for the purpose held, and are kept accurate and up-to-date. Records must be kept 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.

e. Off-site Working

- **Medical Records can only be transferred between Trust sites using Trust Transport, including authorised taxis and ambulances.**
- Medical Records may only be taken offsite if absolutely necessary and on approved business, as authorised by the Head of Medical Records or their agreed Deputy. Please see the **Health Records Policy** on **StaffNet**.
- Other PCD may only be taken offsite 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 **DPA** Principle 7. Ideally this would be in a locked container, but should certainly be something that does not obviously contain PCD.
 - 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.



f. Requests for Information

If you receive a request for information about a patient, staff member, etc. and it is not usually part of your job to respond:

- Refer requests for personal information immediately to your line manager or to the person who is designated to deal with such a request. (See Chapter 6.)
- Refer any enquiries from the police or media to the person designated to deal with such a request. See the **Disclosure of Information to the Police Policy** or pass media requests to the Communications Team during working hours or the On-Call Manager out of hours. (See Chapter 7.)
- Handle enquiries from relatives and friends in accordance with the wishes (consent) of the patient, taking care to identify the enquirer. Effectively, unless a legal exemption applies (e.g. Court Order, Power of Attorney); no-one has the right to information about another person without their explicit, unambiguous consent. This also applies to parents of children who are considered to have the capacity to make their own decisions (13 years or over).
- Guard against people seeking information by deception, in particular, by checking the identity of people requesting confidential information and by following good practice guidelines for dealing with such requests.

g. Abuse of Privilege

- It is strictly forbidden for staff to look at, or seek, 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.
- Information regarding patients or staff cannot be passed onto a third party unless for direct care purposes, with explicit consent or where a legal exemption applies.
- **Seeking out or looking at information or offering to sell information is an offence under the DPA and may attract an unlimited personal monetary fine in Court (see Chapter 3) and / or disciplinary action that may 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.**

h. 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 20.) If in doubt, contact the IG Team.

i. Patient Contacts and Patient Details

- Unless you have consent 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.

j. Transferring PCD

The ICO reports that there have been a number of insecure transfers of information via fax, post and emails and has imposed monetary penalties on organisations who have failed to comply with the **DPA**. In order to prevent this occurring within the Trust, it is the responsibility of each individual member of staff to ensure they follow the basic procedures as outlined in K-R, below.

k. Social Media

Social media has become a worldwide phenomenon. The 2017 Top 10 sites are **Facebook, YouTube, Twitter, Instagram, Google+, Pinterest, Snapchat, LinkedIn, Tumblr and Reddit.**¹ Some simple advice, as member of staff, 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.
- Mix up your work life and private life.



l. Safe Haven Fax Process

The NHS has strengthened an already-existing requirement that fax machines may only be used to transfer PCD when absolutely necessary. If there is no alternative to using a fax, the rules below must apply:

- All PCD faxed between and within NHS organisations must pass between Safe Haven faxes wherever possible or follow the Safe Haven process. These must meet certain security requirements including that:
 - The room or area where the fax is located is lockable and is kept locked at all times when not attended.
 - The room or area should not be an area open to public access. If this is unavoidable, steps should be taken to ensure that no PCD is displayed where it can be seen by members of the public.
 - A manager is identified to take responsibility for the fax machine and ensure that it operates within this procedure.
 - All staff working in a Safe Haven area must have undertaken and passed their mandatory IG Training.
 - All information accepted into the Safe Haven must be handled in a secure manner and only passed on if is required for healthcare purposes or the person receiving the information has been authorised to access it. If there are any concerns about passing information on, advice should be sought from the IG Team.



- All information accepted into the Safe Haven must be dealt with in accordance with the [Confidentiality NHS Code of Practice](#).
- If the nominated member of staff responsible for the Safe Haven fax is on annual leave or absent, arrangements must be made for a colleague to cover for them.
- Switchboard must be informed of any permanent changes so that the list of Safe Haven faxes can be amended accordingly.

If it is not possible to send to a fax that is a Safe Haven, the following must be followed:

¹ 'Most Popular Social Networks in the UK', *Social Media Website*, accessed from <https://social-media.co.uk/list-popular-social-networking-websites>, on 24/08/2017.

- Telephone the recipient of the fax (or their representative) to let them know you are going to send PCD.
- Double check the fax number.
- Use pre-programmed numbers wherever possible.
- Ask them to acknowledge receipt of the fax.
- Always use the Trust's fax coversheet, which is marked "Private and Confidential", and can be found on **StaffNet**.
- Include the total number of pages sent on the cover sheet.
- Request a report sheet to confirm that transmission was received.
- Place faxes received in an envelope with the name of the person the fax is addressed to and the sender written on the front. Mark the envelope "Private and Confidential" and "Urgent", if applicable.
- Contact the intended recipient to let them know that a fax is waiting for them to collect.
- Ask members of staff who frequently receive such faxes to check regularly for faxes addressed to them.

m. 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 the correct letter / document / information is in the correct envelope.



n. Internal Mail

- If using 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 normal 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 the correct letter / document / information is in the correct envelope.

o. Hoax Calls and Emails

There are a continuing number of telephone 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 recent 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. If the caller terminates the call at this point please alert the IG Team using the numbers on the back of this *Handbook* to enable the call to be logged, or
- Discreetly transfer the call through to the IG Team on the same numbers. 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, Sophos, should strip 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 it is not expected or if it is from a company that they have not had any dealings with. Sometimes emails that look genuine maybe hoaxes, looking correct, but for example having one letter missing or replaced. Do not respond to them email or attachments. Just delete it and then remove it from the deleted items folder.

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.

p. Checking a Caller's Identity

To ensure you are speaking to the patient if they call and are asking for information regarding their care, or to update their contact details, GP, etc., you should undertake a three-point identification check, as you would be asked if you called your bank. Doing this demonstrates that you have made best endeavours not to release information inappropriately to someone who should not have it. Examples of the three points of identification that could be asked include, but are not limited to:

- Full name
- Date of birth
- First line of address
- Postcode
- NHS number
- Date of last clinic attended

q. 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
- 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.

The outcome 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 the **DPA** as it inappropriately shared the most sensitive of information. This cost them a fine of £180,000 from the ICO.

r. Confidential Waste and Confidential Waste Bins

Any confidential information, whether PCD or business information, held on paper that is no longer required must be placed in a confidential waste bin. There are different types of bins in different areas. The Waste Management Team can supply one of the following to suit the needs of your Department: a secure cabinet, blue wheelie bins and hessian sacks that fit into red cardboard containers. These are emptied as follows:

- Secure cabinets: weekly, by our external contractor.
- Blue wheelie bin: exchanged on a designated day each week by the waste collections team. (These are used in high-producing areas)
- Hessian sacks: for smaller offices and collected on an as-and-when basis.

The Trust is not only safe guarding confidentiality but being environmentally friendly too. As all our shredded confidential paper is taken to a paper recycling plant and turned into either toilet rolls or egg boxes.

For queries regarding the collection or disposal of confidential waste, please contact:

St Richard's Hospital
x35961

Worthing Hospital
x85178

Southlands Hospital
x83519



Chapter 5: 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 his 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 mother of the child
- The biological father of the child, and
 - Were married to the mother at the time of the birth, or
 - Married the mother after the birth of the child
- The adoptive parents once an adoption order has been made.

Both father and mother will continue to have parental responsibility, even if the marriage breaks down.

Unmarried fathers did not have the same rights and responsibilities as married fathers 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 fathers can only get parental responsibility by:
 - Obtaining a parental responsibility order via the courts, or
 - Completing a Parental Responsibility agreement form with the mother of the child and taking it to a solicitor
- **Children born on or after 1 December 2003**, unmarried fathers can only get parental responsibility by:
 - Obtaining a parental responsibility order via the courts,
 - Completing a Parental Responsibility agreement form with the mother and taking it to a solicitor, or
 - If they are named on the child's birth certificate.

Civil partners of mothers and married lesbian couples; if the child was conceived by artificial insemination on after 6 April 2009 and the mother was in a civil partnership, the civil partner will automatically have Parental Responsibility for the child. Similarly, if the mother is married to their same-sex spouse and the child was conceived by artificial insemination the spouse will automatically have Parental Responsibility for the child. Both names should be added to the birth certificate and the child would have no legal father.

b. What About Non-Parents?

Other people can also acquire Parental Responsibility for a child. These might include step-parents, grandparents or same-sex partners. Non-biological parents can acquire Parental Responsibility if:

- **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 her or his 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 his or her 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 arrangement 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 him or her** – in the 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.
- **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 required signed consent from all parents with Parental Responsibility.
- **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.

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 father and mother must have registered the child's birth together on or after 1 December 2003, or
- Marriage Certificate, OR
- Parental Responsibility Agreement entered into by birth parents, 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**.

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 6: Subject Access Requests

Under the **DPA**, all living individuals or 'Data Subjects' have a right to be informed of the following:

- If the Trust holds, stores or processes PCD about them.
- A description of the PCD held, the purposes for which it is processed and to whom the personal data may be disclosed.
- A copy of any information held.
- To be informed as to the source of the data held.

For Medical Records, SAR Clerks within the IG Team are responsible for dealing with SARs received and to ensure they are responded to in line with the statutory requirement of 40 days. The Trust has robust SAR guidance with agreed procedures to ensure each request receives prompt attention.

Guidance for clinicians is available in a leaflet entitled **Staff Information Sheet: Advice to Clinicians on Requests for Access to Health Records**. Information for patients is also available, entitled **Requesting Your Medical Records: A Guide for Patients** (pictured). Both are on **StaffNet**.

Most of the information released tends to be in 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 for non-medical information may be received in other areas of the Trust, including Human Resources, Estates, Research and Innovation and A&E. They each have local procedures and representatives to deal with requests. Requests for images captured on CCTV are, like other records, managed through the **DPA**.

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 follows:

St Richard's Hospital
subjectaccessrequest.chichester@wsht.nhs.uk
x33181

Worthing and Southlands Hospitals
subjectaccessrequest.worthing@wsht.nhs.uk
x85648

Chapter 7: Sharing Personal Information with the Police

Under the law 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 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 **Section 29(3) Form**. This can be found on **StaffNet** within the **Disclosure of Information to the Police Policy**.

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.



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.

Since April 2010, the ICO has been able to issue monetary penalties to any organisation found to be in breach of the **DPA**. A fine to the organisation of up to £500,000 may be incurred for a serious breach. When new legislation comes about in 2018, the GDPR, this will increase to the equivalent of €20m or 4% of the organisation's annual turnover.

- This is likely to have caused substantial damage or distress.
- Was deliberate or the organisation knew, or should have known, that there was a risk that a breach would occur and failed to take reasonable steps to prevent it.

Each member of staff has the responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way.

- Information lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Information disclosed in error
- Information uploaded to website in error
- Insecure disposal of hardware
- Insecure disposal of paperwork
- Technical security failure, including computer hacking
- Corruption or inability to recover electronic data
- Unauthorised access / disclosure

- Report on Datix, the Trust's incident reporting system, any IG incident of concern.
- Think carefully before sharing PCD without explicit consent, as staff may be held accountable for any unauthorised disclosure.

It is better that a potential incident is reported and discounted later, rather than not being reported and becoming more serious by not being known about.

In principle where a patient or member of staff's information has been breached there is a Duty Candour to let them know. Please discuss this with the IG Team.



Datix can be found on all computer desktops with an orange icon (pictured). If the icon is not present, contact the IT Helpdesk on x85150.

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

It is important not to tell the recipients of incorrect info to destroy it. This is because the Trust need:

- It back to help with the investigation.
- To know for certain that it has been destroyed, and by doing this we only have the recipient's word for it.

Sometimes the recipient of the information may not be willing or able to return it by post or by dropping it back to the Trust. In these situations it is appropriate that someone from the Trust, ideally someone from the Department that mistakenly sent it, goes to collect it.

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

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. This Chapter has been written following broad and ongoing consultation with representatives from relevant staff groups.

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.

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. The IG Team had over thirty concerns notified to them during 2016-17.

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 only the minimal numbers of lists required are produced.
- Ensure 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 use 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.
- 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 so. 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 Professional College or School 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: Decommissioning Work Areas: Checking for Confidential Information

From time-to-time around the Trust 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 sensitive personal data 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 IG Team have produced a Decommissioning Checklist to be completed by any service that is vacating an area of work, which is available on **StaffNet**. 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.

Once completed 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 11: Monitoring Access to Personal Confidential Data

Staff should be aware that electronic systems which access, process or transfer PCD are monitored on a continuous basis.

This is guided by the **IGT**, which mandates that:

Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual [patient] concerned on 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 of individuals and / or the organisation.

Chapter 12: 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 argued 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’ Medical Records are not left unattended.**
- **Locking cabinets and drawers containing confidential information.**
- **Securely storing NHS Smartcards.**
- **Securing key-padded rooms.**
- **Wearing ID swipe cards.**
- **Not leaving confidential papers or waste lying around.**
- **Locking PCs when not using them.**
- **Not writing passwords down.**

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. IT manages the Asset Register for hardware; IG and IT Applications jointly manage the Asset Register for software.

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.

To support this, all staff must:

- Never 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).
- Never 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 the IT immediately.

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.

c. Remote Working and Portable Devices Best Practice Guidance

- 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.

d. USB / Portable Computing Devices

- All USB / portable computing devices, including memory sticks, must be encrypted. USB ports on PCs and laptops are locked down to read only for unencrypted devices.
- 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.

e. Guidelines on Use of USB / Memory Sticks



A memory stick uses 'flash' memory to store data; this is a form of memory that keeps its contents even when unplugged and when power is removed. Memory sticks are a very convenient method for transporting data. Operation is simple, plug the device straight into a computer's USB port and the contents of the device appear as a removable drive that you can drag and drop files into.

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.

f. Destruction and Wiping of Removable Media

If you have removable media that you believe may contain PCD data please return it to the IT Department. All other floppies and CDs with non PCD data on them must be disposed of on a departmental basis. All removable USB memory sticks are to be returned to the IT department for professional wiping.

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

g. Use of Secure Print

- When printing from networked secure printers, it is key that care is used.
- Most staff use their Smartcard 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 13: Use of Email

Email is used by virtually everyone within the Trust 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 the Trust uses the wsht.nhs.uk email domain. **Internally** this is a secure means of emailing. When it is appropriate to transfer PCD external to the Trust, the use of an NHSmail account is necessary. **NHSmail is sometimes called NHS.net; they are exactly the same.** When sending emails with PCD outside of NHSmail users must type **[secure]** in the subject line of the email. 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]**.



Do not email PCD to personal email accounts without the auditable freely given and unambiguous consent of the data subject. If you have any queries, please seek guidance from the IG Team.

As with all communication of PCD, the Caldicott Principles must be adhered to at all times when sending PCD. It is important that you consider carefully if it is necessary to transmit the information at all. Information should only be communicated to people who have a justified reason for receiving the information and no more than absolute minimum of information necessary should be communicated e.g. NHS number rather than name and address.

The recipient's email address should be an appropriate one. For example if sending PCD to a nursing home by secure NHSmail the email address should be either of an appropriate individual or a team email to which only appropriate individuals have access. Sending care plans to a generic admin email address for the care home would not be acceptable even by secure NHSmail.

All emails have the potential to be distributed to anyone. Confidentiality and security should always be considered when handling any information.

Emails containing PCD must be sent in compliance with the Trust's **Information Security Policy** guidelines on email and internet usage and NHS Digital guidance available on **StaffNet**.

Email services are a Trust resource and intended to be used for Trust business purposes. However, some limited personal use is acceptable during breaks / non-working hours.

It is advisable to request a read receipt when sending PCD. If the message is not one that the recipient is known to be expecting consider a preliminary message to check whether the intended recipient is available. Do not send, for example if you get an Out of Office response.

Further general guidance is available in **Faster, Better, Safer Communications: Using Email in Health and Social Care**, published by the Professional Records Standards Body, available from the IG Team.

b. Receiving Secure NHSmail in wsht.nhs.uk Email Accounts

NHSmail users in other organisations may send emails to your wsht.nhs.uk email that contain personal information. If so, you will receive an email with the red



flash (right) in the body of the message. There will also be an attachment that explains the process you must go through to be able to read the email. The attachment will take you through to a webpage. Following the instructions on that page is perfectly safe.

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, 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.

d. Emailing Patients

In 2015 the Professional Records Standards Body made some recommendations about the use of email to communicate with patients. This is that:

- 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.
- 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. Organisations should have clear guidance for patients that can be used to tell them about these possible problems. Patients should have the opportunity to accept this risk before you send any PCD.
- 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, beyond the general agreement to email communication, for example mental-health treatment or sexual-health diagnoses.

Chapter 14: Patients and the Public Taking Photographs

In this highly technological world it is easy to capture a special moment using a camera, mobile phone or tablet, that taking photographs and videos has become almost second nature and done without thought to the wishes of those whose images are being captured.

In a setting such as a hospital ward or department, care must be taken to ensure that the privacy of patients and staff is not compromised.

Whilst many people will feel entirely comfortable with being photographed or videoed it should be recognised that this will not apply to all.

a. Photographs / Videos for Personal Use

Data Protection law does not specifically prohibit the taking of photographs and videos for personal use and for the vast majority of people their images will fall into this category.

If the purpose of the photograph or video is to capture a special event such as a new-born baby this is entirely acceptable. Where this is less clear, however, is when the photograph or video captures staff members or other patients, either by design or accidentally.

Giving due regard to the privacy of the patients and / or staff can be a difficult call to make but usually a polite request to the individual to delete the photograph or video or to possibly reframe it so that no-one else is captured will usually be sufficient.

If a polite request to delete a photograph / video or to stop filming or taking photographs is ignored, staff should first alert their line manager to intervene. If this is unsuccessful, request security assistance as legally we do not have the power to seize the equipment or force individuals to delete a photograph or video.

b. Photographs / Videos Intended for Publicity or Publication

Again, Data Protection law does not prohibit taking of photographs or videos for personal use. However, as it is almost impossible to try and ascertain the intended purpose, it is recommended that a suitable poster be displayed that clearly states that consent may be required. The IG Team have developed a poster for this purpose.

Posting of photographs at work and of patients or their information on social media is clearly unacceptable, especially if the patient or member of staff had previously refused consent to be photographed. There is in reality little that can be done 'after the event' to get photographs or video removed once they appear on

social media sites, unless they can be considered libellous. Trust policy can be applied to staff taking photos but not to the general public.

If a patient or member of staff feels sufficiently strongly about the use of their image on a social media site they may need to get legal advice on the options open to them.

Photographs or videos taken with the intention of publication, for which payment may or may not be received, **must** have the explicit consent of the subject.

c. Photographs / Recordings for Clinical Purposes

This chapter is intended for guidance for photographs and videos taken for personal purposes. The Trust's Consent Policy on **StaffNet** gives guidance on the taking of photographs, videos and voice recordings for clinical purposes.

d. Other Purposes

On rare occasions an individual may take photographs or video for other purposes such as to provide evidence of wrong doing, a health and safety issue or to pursue a complaint against the hospital or individual member of staff.

In these instances security must be involved at the earliest opportunity.

Chapter 15: Information Governance Mandatory Training

Every individual who works for the organisation is required to complete mandatory annual IG training. This includes all new starters, existing staff, temporary workers, volunteers and contractors. The Trust has 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 trust 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 IGSAG 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 the annual Your Health and Safety Update or Mandatory Training Day.
- An e-learning module is available [here](#). (If you are reading a hard copy version of this document, please contact the IG Team for guidance on how to access this module.)
- Bespoke face-to-face sessions are available for specific teams or requirements by contacting the IG Team.



Chapter 16: Records Management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, 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.



Unlike the majority of organisations, the NHS has two categories of records, medical and corporate.

Medical Records can be considered records which contain all patient health records (for all specialties and including private patients, x-ray and imaging reports, registers, etc.).

Corporate Records can be considered records which contain the following administrative records (e.g. personnel, estates, financial and accounting records, 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](#).

a. Manual Records

- Management of the Trust's paper and manual records are guided by the [Records Management Code of Practice for Health and Social Care](#) and the **Health Records Policy** and **Information Lifecycle Policy for Corporate Records**, all of which are on **StaffNet**.
- To ensure the availability and known whereabouts of Medical Records at all times, whenever they are moved between locations they **must** be tracked on SemaHelix using the Patient Document Tracking function, often known simply as PDT.

b. Electronic Records

- Management of the electronic records are similarly guided by the [Records Management Code of Practice for Health and Social Care](#)
- Electronic files should be named accurately and be easy for all to understand. A file structure should be used to ensure that all staff can follow the same filing structure.
- 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.

- All electronic files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived (Zipped in a secure folder).
- Each department should compile a list of standard terms and uniform terminology as naming conventions for files and folders.
- Version controls should be applied and periodically reviewed.
- Records with PCD should be controlled through the use of logins, password protection and encryption.
- Once a project is completed, all associated electronic documentation should be contained in a Zipped file, accurately named / dated and stored within a secure folder on the network. This will decrease storage space and will keep all common documentation together.

Chapter 17: Freedom of Information Requests



The **Freedom of Information Act 2000** (FOI) encourages transparency within the public sector and assumes that openness is standard so that, for example, decisions on how public money is spent or services provided can be seen and understood.

The Trust also produces a Publication Scheme which is available on **StaffNet** and the external Trust website. The scheme includes the following information:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing
- How we make decisions

Management of the Trust's FOI obligations is documented in the **Freedom of Information Policy**, which is on **StaffNet**.

You must not attempt to respond to FOI requests themselves; any queries or requests received must be referred to the FOI Team:

foi@wsht.nhs.uk
x33481

Chapter 18: Data Protection Impact Assessments for New or Existing Projects

It is the responsibility for 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 Data Protection Impact Assessment (DPIA, formerly known as a Privacy Impact Assessment) is a risk assessment tool used by the IG Team on behalf of the Trust to help establish IG implications at the start of a proposal, programme or project.

The **Privacy Impact Assessment Policy** and documentation is available on **StaffNet**.

Identifying IG elements at an early stage will help ensure:



- The aims of the project are met wherever practicable.
- Compliant operations.
- Necessary information sharing protocols are in place.
- Privacy risks are minimised.

It will also eliminate the potential of failing to comply with the **DPA** 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 patient identifiable data 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 patient data. This is achieved by utilising a security matrix.

Chapter 19: 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, compiled 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 process is documented in the **Business Continuity Management Policy**, the **Trust Business Continuity Plan** and individual departmental **Business Continuity Service Level Plans**; these and further documentation are available on the Emergency Planning pages on **StaffNet**.

Chapter 20: Information Sharing

In 2013 a new Caldicott principle was added that promoted the principle 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 Trust must ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.



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

- Purpose for the information to be shared / purpose of the protocol
- With whom the information will be shared
- Appropriate senior endorsement of information sharing protocol
- Structures of sharing information
- Legislation and regulations which are required to be adhered to under the **DPA**



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

1. **A High level Charter and Principle.** The Trust achieves this by being signatory to the Sussex-Wide Information Sharing Protocol, adherence to which is evidenced, by the receiving organisation, through **IGT** Level 2 or other 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 Standard Operating Procedure.** This gives team-level detail regarding how the information will be transferred, by what means and to whom.

For further advice and guidance on ISAs, contact the IG Team.

Chapter 21: 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 be anonymised. 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.



Pseudonymisation within a trusted and safe environment may be an acceptable alternative. This is similar to anonymisation, but means that a unique identifier still exists and that somebody somewhere could link the information back to the real individual if they needed to.

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

- 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 e.g. The Health Service (Control of patient information) Regulations 2002
- 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 appropriate advice. Key guidance includes:

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

Chapter 22: 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 lead. It is up to the Trust's Registration Authority 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 all staff, including temporary / agency / bank and locum employees, 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 IG policies associated documentation and their responsibilities in relation to use of and access to the system.
- 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 theft or misuse of your Smartcard.
- Replacement cards can be obtained by logging a request via the IT Self Service icon.
- 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 suite of IG policies and procedures; adhere to the Data Protection and Caldicott Principles, the [Confidentiality NHS Code of Practice](#) and the Care Records Guarantee.

Chapter 23: Data Quality

The IG Team frequently receive enquiries about how to change information on SemaHelix, 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 responsibility, it is managed for the Trust by the **Data Quality Team**.

The Team's aim is for the Trust to hold the most accurate and up-to-date information on our patients and to make sure that the activity against each patient is recorded correctly. They understand that anomalies and circumstances can sometimes present difficulties for SemaHelix users so are keen for you to call them if you need help.



For more information about Data Quality and relevant information please see the Data Quality pages on **StaffNet**.

For queries regarding Data Quality, please contact the team as follows:

x32195 or x33383
duplicates.semahelix@wsht.nhs.uk

Chapter 24: When Staff Become Patients

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

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, Trust 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 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. 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 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. Confidentiality concerns a telephone containing appointment details being left on a voicemail and being played back in an open plan 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 25: 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 and abuse of position. 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.

Specific examples of fraud include

- **Stolen NHS IDs:** An NHS human resources worker handed over the names of 1,300 employees to a criminal gang. The personal details were used to forge identity documents so that gang members could file multiple applications for benefits at job centres. The gang claimed nearly £500,000 between July 2011 and September 2013. A further £450,000 in claims fell through. The five members of the gang were jailed for a total of 25 years at Southwark Crown Court.
- **Chief Executive Officer Phishing Scam:** Be aware of emails containing urgent payment requests from senior members of staff, accompanied with payment instructions to a specific account. The email is a targeted phishing scam which is enabled through gaining access to senior members' email accounts or emails sent through a recently registered domain name which is very similar to the organisation's email address. A report from the City of London Police's National Fraud Intelligence Bureau shows that over £32 million has been reported to be lost as a result of CEO fraud. From July 2015 until January 2016 there was a marked increase in CEO fraud with nearly 1,000 reports being made to Action Fraud.
- **HM Revenue and Customs Scam:** Fraudsters are sending out virus-infected emails which claim that a package has been seized by HM Revenue and Customs upon arrival into the United Kingdom. The official-looking scam emails, claiming to be from Royal Mail, contain a link to a document which will install malicious software on the recipient's computer designed to steal credentials like account names, email addresses and passwords.

Fraud trends continue to evolve and fraudsters are using ever more sophisticated methods. It is important that you remain vigilant and if in doubt, report your concerns immediately.

If you have suspicions that fraud may be occurring or wish to receive further information about the above, including training, please contact the Trust's Local Counter Fraud Team via their **StaffNet**. Alternatively you can refer to the Trust's **Anti-Fraud and Bribery Policy**. Additionally, you can report any concerns to NHS Protect on 08000 284060 (8am to 5pm, Monday to Friday) or via the online reporting form at www.reportnhsfraud.nhs.uk. All information provided via the secure website is completely confidential.

The Trust has a responsibility to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern.

Chapter 26: Current Affairs

Over the last year there have been several news stories that illustrate what happens when IG in the NHS goes wrong or, indeed, where there is good practice. A selection of these, and other similar stories of interest, is included below, along with links to the full news story on the internet.

It is essential as a Trust that we learn from stories such as these to improve our own processes.



- [Facebook recommended that this psychiatrist's patients friend each other](#)
- [Walsall woman has personal medical records stolen from physiotherapist's car](#)
- [NHS handed over GP data to 150 groups against patients' wishes](#)
- [Former NHS employee fined for illegally accessing patient information](#)
- [DeepMind signs up second NHS trust to health app.](#)
- [Health data breaches on the rise.](#)
- [New national NHS patient "data lake" proposed based on STPs.](#)
- [Shared records starting to make headway.](#)
- [The GP practice sharing data to transform care for homeless people.](#)
- [Fine for IVF company HCA International Ltd.](#)
- [£650 fine for former nurse Elaine Lewis, 63, who 'inappropriately accessed' thousands of patient records across Hywel Dda health board region.](#)
- [ICO investigating GP system supplier TPP over 'data protection compliance concerns](#)
- [NHS data loss scandal has prompted five inquiries, ministers say.](#)
- [Google's Deepmind NHS deal 'inexcusable', says academic paper.](#)
- [Devon doctors' surgery says sorry for data breach.](#)
- [SystmOne creator hits back in row over patient records 'enhanced data sharing' claims.](#)
- [Garages, new homes and old offices: the records management mistakes that put health records at risk.](#)
- [NHS trust employees fell for phishing attack.](#)
- [Public Health England warns of 'serious risk' over Home Office data sharing.](#)
- [Barts Health NHS Trust has canceled 136 operations and hundreds of chemotherapy appointments due to IT failure.](#)
- [Google received 1.6 million NHS patients' data on an 'inappropriate legal basis'.](#)
- [CQC to beef up NHS information governance inspections.](#)
- [Basildon Borough Council £150,000 fine.](#)
- [Should doctors use WhatsApp to bypass archaic NHS tech?](#)
- [Hundreds of patients potentially harmed by undelivered NHS mail.](#)
- [Four lessons NHS Trusts can learn from the Royal Free case.](#)
- [Why are we giving away our most sensitive health data to Google?](#)
- [Doctors resort to sharing patient scans over SNAPCHAT as NHS accused of missing digital revolution.](#)
- [Google's DeepMind Health independent review panel shares first annual report, raises concerns with data privacy and security.](#)
- [Lives could be endangered if we do not protect NHS data securely and ensure it is shared with those working to improve medical care - Lord Darzi.](#)
- [Bupa international health insurance warns of internal data breach.](#)
- [NHS medic posts confidential patient data of new mums on Facebook.](#)
- [NHS patient data serious incidents doubled since Capita contract.](#)
- [London goes live with capital-wide child health information service.](#)
- [Hundreds of sensitive council documents found in London estate.](#)
- [Data on 1.2 million NHS patients stolen, claims hacker.](#)
- [Medical records of Norfolk patients found in a petrol station, a King's Lynn restaurant and on the pavement.](#)
- [ICO warns NHS staff that unlawfully accessing patient records is an offence.](#)

Consultation, Distribution and Acknowledgements

a. Internal Consultation

This *Handbook* was signed off as appropriate for distribution to all staff by the Trust's IG Assurance and Strategy Group on 5 September 2017. In addition to members of that group, several others very kindly reviewed sections relevant to their area of work. These include:

- Andy Banks, Head of Systems Development
- Cathy Coppard, Named Nurse Safeguarding Children
- Mark Dennis, Head of Information Services
- Charlotte Fitzgerald, Freedom of Information Assistant
- Heather Greenhowe, Senior Consultant, RSM UK Tax and Accounting Limited
- Paul Jepp, Portering, Post, Waste, Receipts & Distribution Manager
- Jonathan Keeble, Communications and Engagement Director
- Mark Stevens, Emergency Planning and Business Continuity Manager

I am particularly indebted to 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 Information Governance Assurance and Strategy Group agreed the following distribution process:

- Via a Global email containing a link to the document on **StaffNet**.
- The note within that Global 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 IG colleagues external to the Trust, who have generously shared documents and advice for previous iterations of this document that greatly helped inform the development of the Second and Third Editions. These include Martin Gibson, Sandre Jones, Del Montasir, Jaki Stockwell and Dhiraj Tailor. 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.

Andrew Harvey
Head of Information Governance
September 2017

Notes

[illegible]

This image shows a full page of white paper with horizontal dashed lines, typical of primary school writing paper. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

The Information Governance Team's Mission Statement:

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.

Information Governance Team Contact Details:

Telephone: 01903 205111 x85527, x84588 and x84508, x85402

Email: information.governance@wsht.nhs.uk

Locations: Medical Records, East Wing, Worthing Hospital
and C/o Subject Access Request Team, Medical Records, St Richards Hospital

Format and original material © (2017)