NHS
University Hospitals Bristol
NHS Foundation Trust

Information Governance Induction Training 2018/19

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

Assessment

- The Trust is required to train all staff about Information Governance at Induction

- All staff must complete an assessment either:
  - On paper throughout this presentation
  - Through eLearning in the next 6 weeks

- The pass mark is 80%

What is Information Governance (IG)?

"Information Governance aims to ensure all patient, staff and corporate information is stored, handled and used confidentially and securely."

Why is IG important?

- Patients and staff expect their records to be confidential
- Health records need to be accurate and available to support safe care
- Information needs to be shared appropriately with those who need it

Legal Regulations

The main legal regulations surrounding Information Governance are the:

- Data Protection Act 2018
- Freedom of Information Act 2000

The Information Commissioner's Office (ICO) enforces these regulations in the UK.

Question 1 – Tick one answer:

Which organisation polices the Data Protection Act and the Freedom of Information Act in the UK?

A) The Information Commissioner's Office

B) The Department of Health

C) NHS England

Duty of Confidentiality

Under common law:

- All NHS Staff have a Duty of Confidentiality
- Any information provided in confidence, should not be used or shared further without the individual's consent

Exceptions to Duty of Confidentiality

Consent is not required if there is:

- A legal reason to disclose the information
- A significant public interest in the disclosure

If in doubt – Give IG a shout.

Question 2 – Tick one answer:

Which of these staff groups have a duty of confidentiality?

A) Clinical Staff

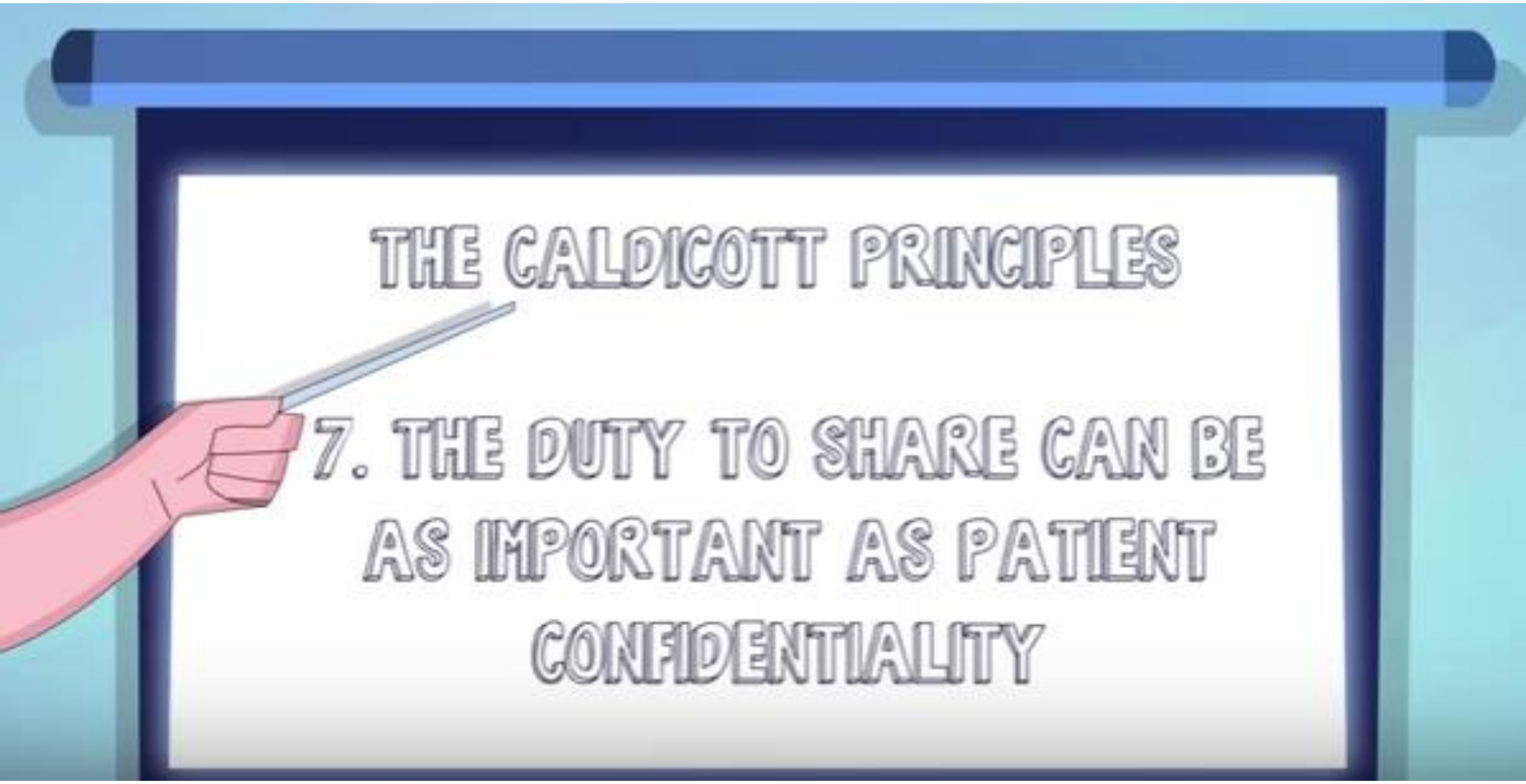
B) Administrative Staff

C) Estates and Facilities Staff

D) All NHS Staff

The Caldicott Principles

- The outcome of a report into how confidential information was used in the NHS.
- The Caldicott Principles provide a framework for using confidential information.


THE CALDICOTT PRINCIPLES
7. THE DUTY TO SHARE CAN BE AS IMPORTANT AS PATIENT CONFIDENTIALITY

Caldicott Guardian

A Caldicott Guardian is a senior member of staff responsible for:

- Protecting confidentiality
- Ensuring records are used and shared properly

Dr Jane Luker is Caldicott Guardian for UH Bristol

Question 3 – Tick two or more answers:

How can you abide by the Caldicott Principles?

A) Complete your training

B) Use confidential data when it's not necessary

C) Never sharing information

D) Only access records you are entitled to

Information Sharing

- Information can be shared for care and non-care purposes
- Clinical staff have a duty to share care information in the patient's best interests
- Sharing for non-care purposes should be checked with the Information Governance Team

Information Sharing for Care

When sharing information for care purposes:

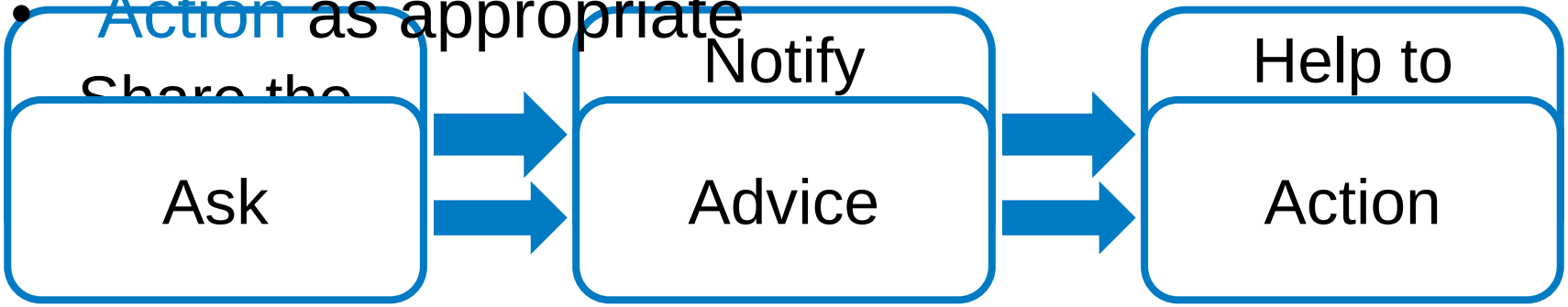
- Check that the individual understands why
- Ensure best practices and policies are followed
- Respect objections the individual may have

Information Sharing for Non-Care

Consent not required in most cases

However, if there is a risk of harm to an individual you should:

- Ask the Information Governance Team for advice
- Take their advice
- Action as appropriate



Question 4 – Tick one answer:

You must get consent from the patient to share their information if:

A) The health & safety of an individual is at risk

B) A company wants the information for non-care purposes

C) There is a legal requirement to share the information

D) The patient is at risk of immediate harm

Information Security

All staff owe a duty of confidentiality to information encountered during their work

There are a range of potential threats to the confidentiality of this information that are either:

Physical

Digital

Physical Information Security

- All confidential paperwork should be stored and disposed of securely
- The volume of paperwork kept on your desk should be kept to a minimum
- Wear your ID badge at all times, and challenge those without one in your ward/department

Digital Information Security

Social Media

Before posting on social media you must consider:

- The audience of your post
- How it may be perceived
- How it may affect our reputations
- Potential to go viral

Question 5 – Tick all that are correct:

Which of the following increases the security of information?

A) Using confidential waste bins

B) Leaving your PC unlocked and unattended

C) Keeping lots of paperwork on your desk

D) Challenging individuals with no ID badge

E) Deleting suspicious emails

Information Governance Incidents

Any breaches of confidentiality must be reported as Information Governance Incidents as soon as you are aware of them.

All staff should be able to:

- See activities where information could be lost
- Know what needs to be reported
- Improve the security of information in their area

Types of Incidents

The most common incidents in our Trust are:

- Letters sent to the wrong address
- Letters for multiple individuals sent in the same envelope
- Dropped handover paperwork

Reporting Incidents

All incidents across the Trust are reported on Datix.

Datix can be accessed on any Trust PC and any member of staff can report incidents.

Datix can be found in the “Top 10 Links” on the front page of connect.

Question 6 – Tick all that are correct:

Which of the following statements about Information Governance Incidents are true?

A) They aren’t important

B) They involve a breach of confidentiality

C) You only report serious incidents

D) You can wait a week to report them

E) They must be reported on Datix

Records Management

The Trust is required to ensure all information is:

- Accurate
- Relevant
- Up to Date

Most of all however, information has to be:

- Available

Managing Records

All records must be:

- Logically named
- Version controlled
- Stored safely
- Traced accurately
- Secured
- Appraised

Question 7 – Tick one answer:

When sending or receiving hospital notes, what is the first thing you should do?

A) Put them in a drawer

B) Leave them unattended

C) Trace the notes correctly

D) Phone the sender to thank them

Record Keeping

Poor quality information is a risk to patients, staff members and the Trust.

All staff need to:

> “Clearly record the correct information, on the correct record, in the correct system”

Clinical Record Keeping

When working with clinical records, there are other responsibilities:

- Records should be free from duplication
- Record at the time the event occurs
- Comply with any storage and security procedures

All clinical records must contain the individual's NHS Number

Question 8 – Tick all correct answers:

Poor quality information could be:

A) Inaccurate

B) Out of Date

C) Missing an NHS number

D) A risk to patients

Freedom of Information Act 2000

The Act provides public access to information held by public authorities.

If an organisation spends public money, then it is duty bound to respond to FOI requests.

There is a 20 working day turnaround on all FOI requests

Freedom of Information Requests

Any individual can make a request but they have to:

- Provide the request in writing
- Provide contact details

Send all requests to:
FreedomOfInfo@UHBristol.nhs.uk

Subject Access Requests

Individuals have the right to request all information an organisation holds about them.

These requests are handled by appropriate teams:

- Staff information – HR
- Patient information – Medical Records
- High profile cases – Trust Secretariat

Question 9 – Tick one answer:

The turnaround for Freedom of Information requests is:

A) 30 days

B) 4 weeks

C) 20 working days

D) 20 days

Privacy Notice

Provides transparency to individuals about how UH Bristol collects and uses their information.

- All staff must be able to signpost individuals to our Privacy Notice

- http://www.uhbristol.nhs.uk/about-us/privacy/

Further Information

- Information Governance Connect Pages
- Freedom of Information Connect Pages
- IG and FOI Policies and Procedures
- “What we do with your information” leaflet

Your Responsibilities

- Recognise where information may be at risk
- Report IG incidents and near misses
- Complete your annual training
- Know where the Trust's Privacy Notice is

Question 10 – Tick one answer:

The page stating how we collect, share and use individual's data is known as a:

A) Information Statement

B) Privacy Notice

C) Confidentiality Clause

D) Data Usage Report

Marking

- Pass your tests to the next table/aisle
- If the answers given are not what is on the slide, then the question must be marked wrong
- Tick correct answers, and cross incorrect answers

Marking

University Hospitals Bristol
NHS Foundation Trust

9) The turnaround for Freedom of Information requests is:

A) 30 days ☐
B) 4 weeks ☐
C) 20 working days ☒
D) 20 days ☐
E) Deleting suspicious emails ☐

10) The page stating how we collect, share and use individual's data is known as a:

A) Information statement ☐
B) Privacy Notice ☒
C) Confidentiality Clause ☐
D) Data Usage Report ☐
E) They must be reported on Datix ☐

Test Scores

- Your tests will be checked by the Information Governance Team
- Scores will be uploaded to your training record
- Any score below 80% is non-compliant and you will need to complete the e-Learning

NHS
University Hospitals Bristol
NHS Foundation Trust

Information Governance eLearning 18/19

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

Learning Objectives

S – IG training compliance

M – 80% or more in the assessment

A – Answers to the assessment are in the eLearning

R – NHS requirement to train all staff in IG annually

T – 30 minute eLearning, compliance lasts for 1 year

NHS
University Hospitals Bristol
NHS Foundation Trust

Information & The Law

Your Duty of Confidentiality

Access to Information

Click a category to begin:

Sharing Information

Records Management

Information Security & Incidents

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

What is Information Governance (IG)?

"Information Governance aims to ensure all patient, staff and corporate information is stored, handled and used confidentially and securely."

Why is IG Relevant to me?

All staff, students and volunteers encounter confidential information in their role at the Trust

All of our patients and staff expect the information we hold to be confidential

Laws Affecting IG

Data Protection Act 2018	Freedom of Information Act 2000
Regulates the use of personal information	Allows access to information already held by public authorities
Gives individuals rights to access and correct their information	Requests can only be made in writing
Fines of up to €20 Million if the act is breached	There is a 20 working day turnaround for all FOI requests
The Trust must inform people how their information is used	Personal information can not be requested

The Information Commissioner's Office regulates these laws within the UK

Types of Information

Personal - Information that either identifies an individual or is about an identifiable individual

Confidential - Information provided in confidence by the individual, this includes name and addresses as well as healthcare information

Pseudonymised - Information where an individual's identity is disguised using a unique identifier

Anonymised - Information that does not identify an individual, nor can their identity be easily determined

NHS
University Hospitals Bristol
NHS Foundation Trust

Your Duty of Confidentiality

We all have a duty to maintain the confidentiality of information we come across

This extends outside of the hospital grounds

Public transport and cafes are not suitable for work discussions

Your Duty of Confidentiality

You must gain consent if you wish to disclose any information provided in confidence, unless:

If you have any questions, contact InformationGovernance@UHBristol.nhs.uk

Information Sharing

University Hospitals Bristol
NHS Foundation Trust

Personal information can be shared for care and non-care purposes:

Care

Non - Care

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

University Hospitals Bristol
NHS Foundation Trust

Information Sharing for Care

We have a duty to share information to support our patients' care.

When sharing information for care purposes, follow these steps:

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

University Hospitals Bristol
NHS Foundation Trust

Information Sharing for Non-Care

Non care purposes include:

- Marketing
- Research
- Prevention of crime

In most cases, you must gain the individual's consent before sharing information for these purposes.

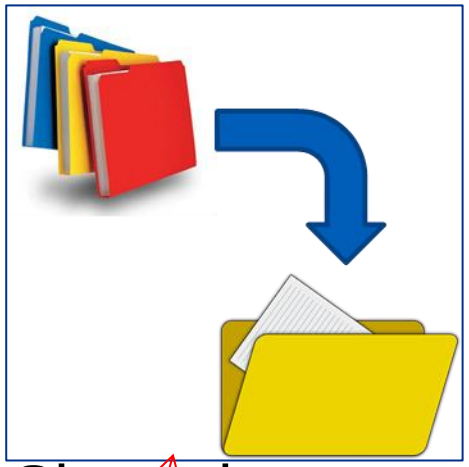
If an individual is at risk of immediate harm then you should share the information and notify the IG team.

Information Sharing Best Practices

Under normal circumstances, you should:

Share information securely

Consider if the recipient authorised to receive such information?



Share the minimum necessary information.

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Sending Information

Information should always be sent securely, secure methods of sending are:

- Post
- Secure email

Faxing information is insecure and should only be relied upon in emergencies.

Sharing Information

University Hospitals Bristol
NHS Foundation Trust

When sharing information either face to face or over the telephone, you should consider the following:

- Is the recipient who they say they are?
- Is the recipient entitled to the information?
- Are you authorised to share the information?

If leaving a voicemail, don't assume that the recipient is the only person who can access it.

Information Security

University Hospitals Bristol
NHS Foundation Trust

There are a range of potential threats to the confidentiality of information through the organisation:

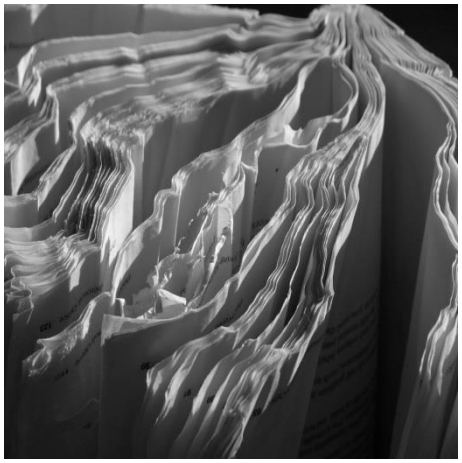
- Physical
- Digital

Physical Information Security

Threats to physical records include:

Loss

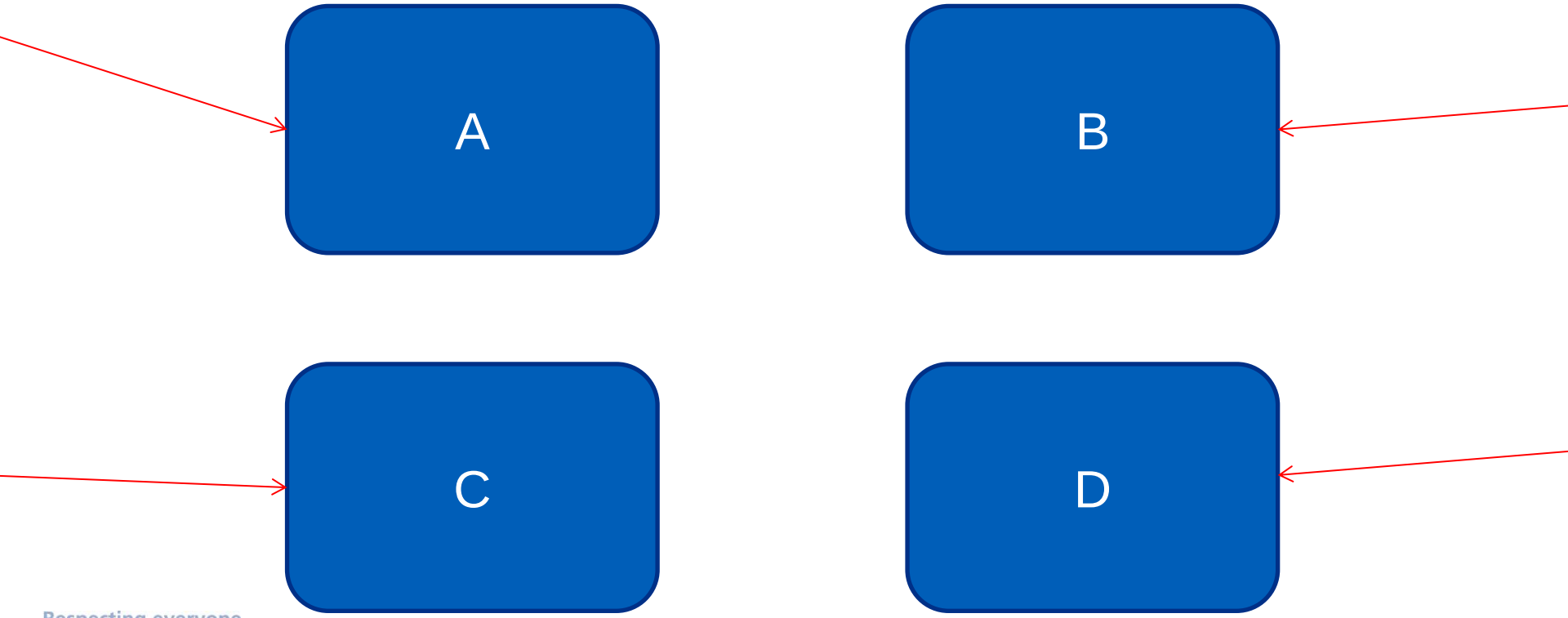
Theft



Damage

Best Practices

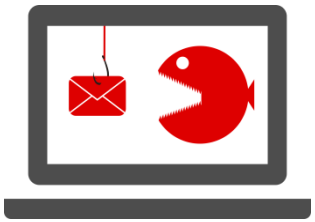
These best practices reduce the risk of loss, theft or damage to our records:



University Hospitals Bristol
NHS Foundation Trust

Digital Information Security

Otherwise known as cybersecurity. These are threats you need to consider when using Trust IT equipment.



Phishing Emails

Ransomware

Social Media

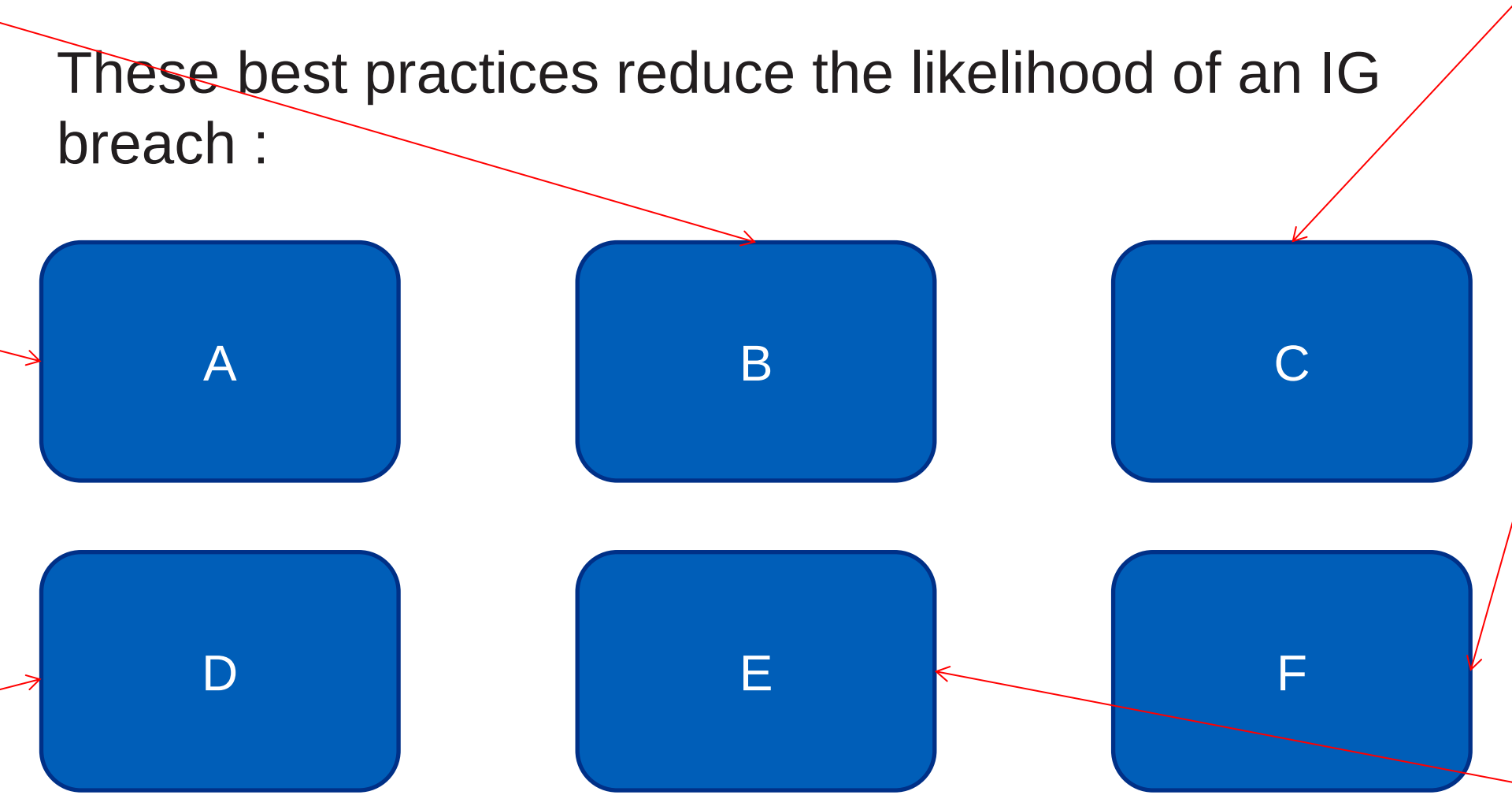
Account Sharing

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

Best Practices

These best practices reduce the likelihood of an IG breach :



IG Incidents

An IG Incident involves a breach of confidentiality, insecure or lost information, or cyberattacks such as malware.

All IG incidents must be reported on Datix as soon as you are aware of them.

Serious incidents are reported to the Information Commissioner's Office

Datix®

IG Incidents

The most common incidents across our Trust are:

- Dropped confidential paperwork
- Records filed in the wrong patient's notes
- Unauthorised access to our IT systems through password sharing or accessing friends, family or your own records
- Confidential information sent insecurely

Records Management

The Trust is required to ensure that all information is:

- Accurate
- Relevant
- Up to Date
- Available

Record Keeping

University Hospitals Bristol
NHS Foundation Trust

All staff need to:

"Clearly record the correct information, on the correct record, in the correct system."

This covers patient notes, training records, equipment maintenance and housekeeping logs.

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

NHS
University Hospitals Bristol
NHS Foundation Trust

Clinical Record Keeping

All clinical records must:

- Contain the patient's NHS Number
- Be free from duplication
- Be recorded at the time the event occurs or soon after
- Be stored securely and traced accurately on Medway

Data Quality

The Trust needs high quality information in order to support safe care and effective decision making.

Any missing, incomplete or incorrect information is poor quality information.

Poor quality information is a risk to patients, staff members and the Trust.

Access to Information

Individuals can request information from the Trust in two ways:

- Freedom of Information Requests
- Subject Access Requests

The Freedom of Information Act

The Act provides public access to non-personal information already held by public authorities.

If an organisation spends public money, then it is duty bound to respond to FOI requests.

There is a 20 working day turnaround for all FOI requests.

University Hospitals Bristol
NHS Foundation Trust

Freedom of Information

Any individual can make a request as long as:

- They provide the request in writing
- They provide sufficient correspondence details

Personal information is exempt from disclosure under the Act.

FOI requests are dealt with by the FOI team at THQ

FreedomOfInfo@UHBristol.nhs.uk

Respecting everyone
Embracing change
Recognising success
Working together
Our hospitals.

Transforming Care

NHS
University Hospitals Bristol
NHS Foundation Trust

Subject Access Requests

Under the Data Protection Act, individuals have the right to request copies of all information an organisation holds about them.

These are known as Subject Access Requests.

This can include their medical records, personnel files and even emails written about them.

University Hospitals Bristol
NHS Foundation Trust

Subject Access Requests

Copies must be provided free of charge, and within 1 month of receiving the request.

Various checks are built into our process to ensure:

- Information about 3rd parties such as family members is removed
- The information is assessed to see if could cause serious harm to the requester

University Hospitals Bristol
NHS Foundation Trust

Subject Access Requests

These Subject Access Requests are handled by appropriate teams across the Trust:

- Staff Information – Human Resources
  EmployeeServices@UHBristol.nhs.uk
- Patient Information – Medical Records
  AHR@UHBristol.nhs.uk

Assessment

Which of the following statements on the types of information used in health and care is correct? Tick one option from the answers listed below.		
A	Personal information applies only to living people	
B	Personal information applies only to patients	
C	A person's name and address are needed for them to be identified	
D	An unusual name will not identify an individual	
E	Anonymised information cannot be personal or confidential	

Assessment

Which of the following statements on the Data Protection Act 2018 is correct? Tick one option from the answers listed below.		
A	The Act only applies to patient or service user information	
B	The Act only applies to personal information in digital form	
C	The Act prevents information being shared for health and care purposes	
D	Organisations can be fined or face legal action for breaching the principles of the Act	

Assessment

Which of the following statements on the Freedom of Information Act is correct? Tick one option from the answers listed below.		
A	The Act puts a duty on organisations to supply information to individuals who make a written request	
B	Individuals can submit a request for information in writing or over the telephone	
C	Organisations must respond to a valid request within 10 working days	
D	If necessary, organisations have a duty to create new information in order to meet a FOI request	

Assessment

Which of the following is the correct turnaround time for Freedom of Information Requests? Tick one option from the answers listed below.		
A	30 days	
B	20 days	
C	20 working days	
D	1 month	

Assessment

Which of the following statements in relation to Subject Access Requests is correct? Tick one option from the answers listed below.		
A	There is no time limit to respond to the request	
B	Anyone can request all information we hold about them	
C	Emails are exempt for the request	
D	Individuals need to pay to receive the copies	

Assessment

Which of the following statements on the topic of confidentiality is correct? Tick one option from the answers listed below.		
A	It is not necessary to explain how someone's personal information will be used	
B	It is not necessary to give them a choice about how their personal information is used	
C	Information can be discussed with friends and family	
D	Information can be shared without consent in some circumstances	

Assessment

Which of the following should not be used to send personal information unless absolutely necessary? Tick one option from the answers listed below.		
A	Post	
B	Email	
C	Fax	
D	Telephone	

Assessment

Which of the following is likely to increase the risk of a breach when sending personal information? Tick one option from the answers listed below.		
A	Using a trusted postal courier service	
B	Verifying the identity of telephone callers	
C	Using a secure email system	
D	Leaving answerphone messages	
E	Encrypting any personal information	

Assessment

Which of the following represents an example of good practice in physical security? Tick one option from the answers listed below.		
A	Having a sign-in procedure for visitors	
B	Sharing your ID badge with a colleague who has forgotten his	
C	Propping open fire doors when the weather is warm	
D	Leaving service user records on your desk in case you need them later	

Assessment

Which of the following statements best describes how to respond to an Information Governance incident? Tick one option from the answers listed below.		
A	All incidents should be reported	
B	An incident should be reported only if it results in personal information being revealed	
C	An incident should be reported only if it results in personal information being lost	
D	An incident should be reported only if it results in harm to a service user	
E	There is no need to report an incident	

Assessment

Which of the following is least likely to create a security risk? Tick one option from the answers listed below.		
A	Leaving sensitive documents on your desk	
B	Using an approved, encrypted USB at work	
C	Using an unauthorised mobile phone for work matters	
D	Leaving a restricted access door open	

Assessment

Which of the following is the best course of action if you receive a phishing email? Tick one option from the answers listed below.		
A	Reply to the email	
B	Forward the email to your colleagues	
C	Delete the email from your inbox + deleted items folder	
D	Open the attachments	
E	Click on the links in the email	

Assessment

Which of the following represents an example of good practice in data security? Tick one option from the answers listed below.		
A	Attaching unauthorised equipment to your work-provided digital asset	
B	Installing updates to your work-provided digital asset as soon as they available	
C	Using your work-provided digital asset for personal reasons not consistent with your organisation's policy	
D	Downloading software or data from the Internet to your work-provided digital asset	
E	Connecting your work-provided digital asset to an unknown network	

Assessment

Which of the following represents an example of good practice in record keeping? Tick one option from the answers listed below.		
A	Storing commonly used records in your drawer	
B	Including each person's NHS number	
C	Creating duplicate records for each person	
D	Preventing people from checking their own details	
E	Updating records at the end of each month	

Assessment

Which of the following represents an example of good Data Quality? Tick one option from the answers listed below.		
A	Incomplete information	
B	Missing information	
C	Incorrect information	
D	Up to date information	

Your Responsibilities

University Hospitals Bristol
NHS Foundation Trust

- Maintain the security and confidentiality of all information encountered in your role
- Only access records that are necessary for you to complete your role
- Report IG incidents and near misses on Datix
- Complete IG training annually
- Be vigilant against social engineering and cyber threats

University Hospitals Bristol
NHS Foundation Trust

Further Information and Contacts

For further information, please try:
http://connect/aboutus/CorporateGovernance/informationgovernance/Pages/default.aspx

If you have any further queries then please contact:
InformationGovernance@UHBristol.nhs.uk

A **simple** guide to

NHS
University Hospitals Bristol
NHS Foundation Trust

General Data Protection Regulation

WHAT IS GDPR?

WHAT REMAINS THE SAME?

WHAT HAS CHANGED?

WHAT DO I NEED TO DO?

FURTHER INFORMATION

What is GDPR?

GDPR becomes law across the European Union (EU) on 25 May 2018.

The new legislation ensures that personal information is handled appropriately and securely by organisations. It builds on previous legislation to bring data protection legislation into line with new, previously unforeseen, ways that data is now used.

Like all other organisations, UH Bristol has a legal duty to follow GDPR when gathering, storing, sharing or processing individuals' data, and we are working hard to ensure we are prepared for the introduction of updated data protection laws on 25 May 2018.

What remains the same?

The good news is that the underlying law has not fundamentally changed.

As before, data protection laws ensure that all organisations handle personal information appropriately and securely. GDPR, like previous legislation, protects individuals' confidentiality. For this Trust and all our patient-facing or other services, that means any person for whom we hold personally identifiable information. Personally identifiable information is any data that could potentially identify a person or any information that can be used to distinguish one person from another, for example someone's name, address, email, NHS number, medical or treatment information, or a photograph.

As before, we must make information available about what personal identifiable information we collect and process. This will explain, for example, what information we collect on patients, and whom we share it with, in order to manage and deliver care to them.

What has changed?

There is a lot more detail in the updated legislation than there was before:

- **Patients, staff and anyone else for whom we hold personal identifiable data has an enhanced right to access their information**, and new or enhanced rights to rectify or ask that the information we have on them is erased (often referred to as "the right to be forgotten") or to restrict or object to the Trust processing their information. However, for patients and staff members these rights are limited because, as a care provider we have a legal duty to keep a full medical record, and as an employer we must keep records under employment law.
- **The Trust must provide more information than before** about what information we collect and process and the legal basis on which we do this; information about individuals' rights, how to complain to the Information Commissioner's Office and how long the Trust holds the information. Most of this is provided in the Privacy Notice on the Trust website.
- **We must draw individuals' attention to information about what data we collect and how we use it**, particularly, for example, when a new staff member starts working for the Trust or when a new patient comes for an appointment.

Continued....

What has changed?

- **If there is no other legal basis on which to obtain or process personal information** we must ask individuals to "opt-in" and provide clear consent. In the past, it was sufficient to ask people to "opt out". The new law means that, for example, if you are collecting contact details of interested members of the public to join a mailing list and work with you in the future, you must obtain a clear opt-in, which cannot be a pre-filled check box, and tell them of their right to change their mind.
- **We must ensure that data protection is built into any new process or changes we make to how we process information.** This is done by an impact assessment that must be completed for all new processes or changes to existing processes which involve personal data.
- **The Trust is required to have a dedicated Data Protection Officer (DPO)** who has a measure of independence and advises the Trust on compliance issues. Our DPO has been appointed.

What do I need to do?

Covering the basics
Ensure that you remain up-to-date with your information governance training.

Communication with anyone whose confidential information we hold
Review all patient, staff or other service user communications which tell people what we do with their personal data. In particular make sure that at some stage in the "conversation" they are being referred to the Privacy Notice on the Trust's website.

New or changed processes within your team
Ensure that you complete a data protection impact assessment for all new procurement, commissioning and service changes which involve the use of personal data.

Access to confidential information
Carefully think through what personally identifiable information you and your team have access to.

Make sure that access to any personal data for which you are responsible is properly managed and only those with a "need to know" have access. This includes information systems and databases, shared drives and other information assets. In your team there should be clear documented procedures for identifying who needs access and for adding and removing their access rights.

The Trust will be issuing further guidance in this area but it is your responsibility to ensure appropriate controls are in place within your area.

If you have any questions about whether there is a legal basis for any activity involving the use of personal data contact the Trust's Data Protection Officer.

Other communication within your team
Carefully consider whether your team uses any mailing lists to contact patients, staff or others. There are stringent requirements on the use of consent and on using email (or SMS) for "marketing" – and the definition of marketing can be very broad, including possibly keeping people updated about services. If you have any doubts as to whether you obtained a clear positive indication of consent (opt-in) when creating your mailing list, and told them that they could change their mind at any time, contact the Trust's Data Protection Officer.

Summary

General Data Protection Regulation (GDPR) becomes law across the EU on 25 May 2018.

It builds on previous legislation to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

UH Bristol has a legal duty to follow GDPR when gathering, storing, sharing or processing individuals' data.

Ensure that you remain up-to-date with your information governance training.

Carefully think through what personally identifiable information you and your team have access to.

Make sure that access to any personal data for which you are responsible is properly managed and only those with a "need to know" have access.

If you have any questions about whether there is a legal basis for any activity involving the use of personal data contact the Trust's Data Protection Officer.

Review all patient, staff or other service user communications which tell people what we do with their personal data.

Carefully consider whether your team uses any mailing lists to contact patients, staff or others.

Further information

More information, including a guide to GDPR for leaders, can be found on Connect at
connect/aboutus/CorporateGovernance/informationgovernance/Pages/gdpr.aspx

The UH Bristol Privacy Notice can be found on our public website at
http://www.uhbristol.nhs.uk/privacy

If you have any questions about GDPR please email
informationgovernance@UHBristol.nhs.uk

A simple guide to...

University Hospitals Bristol NHS
NHS Foundation Trust

Information Governance

In this edition of Simple Guides we explore the issue of protecting confidential patient information.

All NHS employees are duty bound to uphold the principles of the Data Protection Act. This important legislation underpins how we manage confidential information. It's a key part of your employment contract with the Trust, and is a requirement of clinical registration bodies, such as the Nursing Midwifery Council (NMC) and the General Medical Council (GMC). The Trust must also satisfy its information regulator, the Information Commissioners Office (ICO), that we are managing patient information in an appropriate manner.

A simple guide to...

Information governance

Why is information governance important?

Maintaining a high degree of professionalism with regard to managing patient information is a vital component to the care we deliver. Information must reach the right people so that effective clinical decisions can be made; but information must also be protected from inappropriate access, so that patients can be assured that their very personal details are not being misused. If patients didn't have confidence in our ability to manage their information appropriately they would be less inclined to share their details with us, which could impact on our ability to deliver the right care to them.

How can we improve information governance day-to-day?

Here are some suggestions on improving Information Governance (IG) in your role:

- Some basic understanding of the Data Protection Act is required to work at the Trust. This requirement is covered in your employment contract and is also covered in the Trust's induction session and in the annual mandatory training updates.
- Do not share patient information with anyone else unless they have a legitimate professional reason for needing to know. If you are sharing information with a third party there are rules that govern when it is appropriate or not to send information to them. See the confidential patient data sharing policy on the DMS.
- Minimise the amount of information you share, especially with third party organisations that aren't involved in the direct care of our patients. For example, if it isn't necessary to share the patient name, don't. Just use the patient Trust "T" number and date of birth.
- All staff must undertake their essential IG training which is available on the Learning and Development portal. This module is 15 minutes long and covers the basic IG knowledge you need as an employee of the Trust. This essential training should be retaken every year.
- It's important to be aware that the Trust has polices regarding how we manage information. You can find all you need on the IG pages on Connect: type 'information governance' into the Connect search box to find the Trust's IG pages.
- Depending on your role, there are other organisations that will have an interest in your conduct. For example, if you are a nurse, the Nursing Midwifery Council (NMC) has IG guidance and advice you should be aware of.
- The Information Commissioners Office (ICO) is the overarching regulator for the Trust. Their website is an excellent source of data protection guidance (www.ico.uk).
- As a general guide, it's helpful to treat other people's information as though it were your own. A good test is to ask yourself: if this was my information how would I feel about it being shared in this way?
- If in doubt, ask an experienced colleague or contact the information governance officer for the Trust. The contact details for the IG officer can be found on the IG Connect pages.
- If you become aware of an incident involving an information governance breach you should report the incident on the Trust incident reporting system. This system is called Datix and can be found on the Connect home page.
- You can find more information about IG on the relevant Connect pages or by reading the Trust's IG policy which you can find on the DMS (Document Management System).
- Anything a member of staff writes is disclosable so staff should be mindful of what is written in emails and clinical notes. This is because the Freedom of Information Act and the Data Protection Act impose a legal obligation to disclose this information if requested to do so by a legally authorised person (such as the patient or guardian of a patient).

What sort of situations should staff be mindful of?

The organisation must protect the information we are entrusted with in order to function. If we didn't, our patients and our regulators would soon lose faith in us. The Data Protection Act makes it clear we must take all reasonable steps to ensure the information we manage isn't accidently or deliberately compromised.

Confidential patient information is routinely used in a number of situations at the Trust, and staff need to manage these situations appropriately as there is the potential for serious breaches of confidential patient information if the correct practice is not followed:

Taking confidential records off-site

Trust staff deal with very sensitive patient information day-to-day. It's easy to become relaxed about the data we are responsible for. Patient information in physical records should only leave Trust premises if absolutely necessary. Do not take patient information off Trust premises out of habit.

Your workflow must support the Data Protection Act principles, so please consider the reputation of the organisation and your own obligations to uphold the Act.

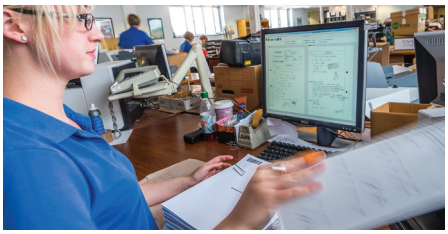
If the management of patient information off Trust premises or between sites is necessary:

- Do not travel with confidential information on unprotected loose sheets of paper or use insecure means of storing it during transit. A secure sealed folder with no open sides or suitable strong case is recommended.
- Do not leave the information unattended at any point in your journey;
- Do not allow unauthorised persons to see the information (this includes other Trust staff who are not involved in the care of your patients);
- Do not travel with confidential information on public transport if possible;
- Return the information to Trust premises as soon as reasonably possible;
- All confidential information to be disposed of must be disposed of in confidential waste bins only.

Mobile phones and personal IT equipment

All staff have an obligation to ensure that electronic confidential data is not stored or transmitted insecurely. **It is not permissible to use unauthorised equipment to store confidential patient information.** This includes the storing of patient identifiers such as names and NHS numbers. The Trust provides a vast range of IT equipment for staff to do their work. All Trust owned equipment is encrypted, tagged, and protected by a multiple range of other security measures. Personal equipment is not protected to this extent and therefore the Trust cannot provide any assurance to our patients that these devices are secure. It is therefore Trust policy to only use authorised equipment to store confidential data. If you want to use your own equipment to receive emails, you need to contact the IT helpdesk and they will assist you.

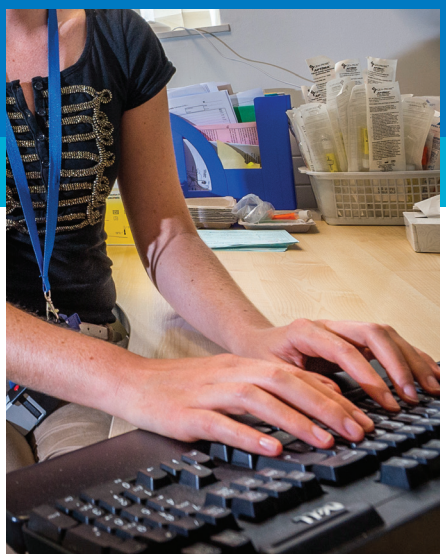
Accessing records appropriately



A fundamental aspect of the work of the staff at the Trust is to access the Patient Administration System and other systems supporting clinical and administrative care. However, having the ability to access data does not give anyone the automatic right to see it.

Staff are only permitted to access records as a direct requirement of their role. Staff should only access patient data if they have a legitimate professional reason to do so. Staff must not access the records of patients they have no professional involvement with, nor must they access their own records, nor the records of family members, friends, partners, or anyone who is not under their care. IT systems are audited and all access can be retraced and investigated. If a member of staff is discovered to have accessed data inappropriately they risk disciplinary action.

If you are performing administrative support to a team, then the same rule applies: you must only access records that you are required to as part of your role at the Trust. Being related to a person or knowing them personally does not give anyone the right to breach a patient's confidentiality.



Emailing confidential information

There are many aspects of emailing confidential information to be wary of. In particular, staff should be careful not to email patient information across insecure networks or to insecure email addresses without the express consent of a patient. When emailing from a UH Bristol email account to another UH Bristol email address, the data is being transmitted within our own network and is secure. However, if you were to email another Trust or organisation, or private email address, the data is moving out of our control and can be intercepted. Emailing patient identifiable data outside of the Trust's email systems is therefore considered insecure unless the appropriate guidance is followed (see the guidance documentation on the IG Connect pages).

The simplest way to transfer confidential patient information/ patient identifiable information is to use an NHSmail account (e.g. fred.bloggs@nhs.net). With an NHSmail account you can securely email another user who also has an NHSmail account, so you can transfer any appropriate and necessary patient information. Both the recipient and the sender need an NHSmail account to ensure that data is shared securely. NHSmail accounts can be transferred between NHS organisations, so you can retain your NHSmail account even if you leave your employment with the Trust and go to work with another NHS organisation.

You can use your Trust email account to send confidential data to an email address outside the Trust, but you need to activate the encryption feature of the email system. To do this you need to add the command [secure] into the subject line of the email. This is explained in more detail in the appropriate guidance document on the Trust's IG pages.

It is also advisable not to send emails to multiple recipients outside of the Trust unless it is absolutely necessary, especially if private email addresses are involved. If you absolutely must send an email of this nature, ensure you understand the correct process to do this and have agreed this with your manager. You must 'blind copy' (referred to as 'Bcc…' in Outlook). If you don't do this all the recipients will have the email address (and therefore the contact details) of all other recipients.

Such circumstances can lead to serious breaches of Information Governance and have led to ICO investigations in other Trusts.

Only send emails to multiple recipients outside the Trust if you absolutely must do so and you understand how to do this correctly.

Training

IG training is essential and must be done annually. Staff can access IG training on the Learning and Development portal. You will find a link for Learning and Development on the Connect home page. Follow the guidance on these pages to gain access to essential training. Once you have gained access to your online training programme, you will be able to do your IG eLearning module. The module is very short (15 mins). There is a short test at the end of the module. Once you've passed this your training record will be updated automatically.

Top tips to remember

1. Do your mandatory information governance training on the Learning and Development portal.
2. Ensure you have a basic understanding of the Data Protection Act.
3. Ask an experienced colleague or contact the Trust's information governance officer if you are unsure what to do in respect of handling patient data.
4. If you become aware of an information governance breach, ou should report the incident on the Trust's incident reporting system, called Datix.
5. Only access information you have legitimate right to access.
6. Ensure any emails that contain confidential data are secure.
7. Do not use personal IT equipment to store or transmit confidential data.
8. Be mindful when transporting confidential information that this information should be protected adequately at all times.
9. You can find the Trust's IG policy and the confidential patient data sharing policy on the DMS via the Connect home page.
10. All written notes and emails are potentially disclosable.

To find out more about information governance, a useful place to go is the Information Commissioners' Office website. They have an excellent guide to the Data Protection Act. The web address is: www.ico.org.uk

University Hospitals Bristol NHS
NHS Foundation Trust

Standard Operating Procedure

SUBJECT ACCESS REQUEST PROCEDURE – OTHER THAN HEALTH RECORDS

SETTING Trust-wide for requests for access to personal data falling outside of the 'Access to Health Records Procedure'

FOR STAFF Staff responsible for handling subject access requests (SAR) other than medical records. Only staff with appropriate training should use this procedure.

ISSUE This procedure details the standard process that should be followed within University Hospitals Bristol NHS Foundation Trust (the Trust) to ensure a consistent approach when dealing with requests by an individual or someone acting on their behalf for access to their own personal information other than health records. It supports the Trust's Information Governance and Data Protection Policies and should be read in conjunction with those policies and the subject access guidance.

Introduction

Article 15 of the General Data Protection Regulation 2016 (GDPR) gives any living individual a right of access to any personal information that an organisation is holding about them and to be given information about how it is dealt with. This is known as a subject access request (SAR).

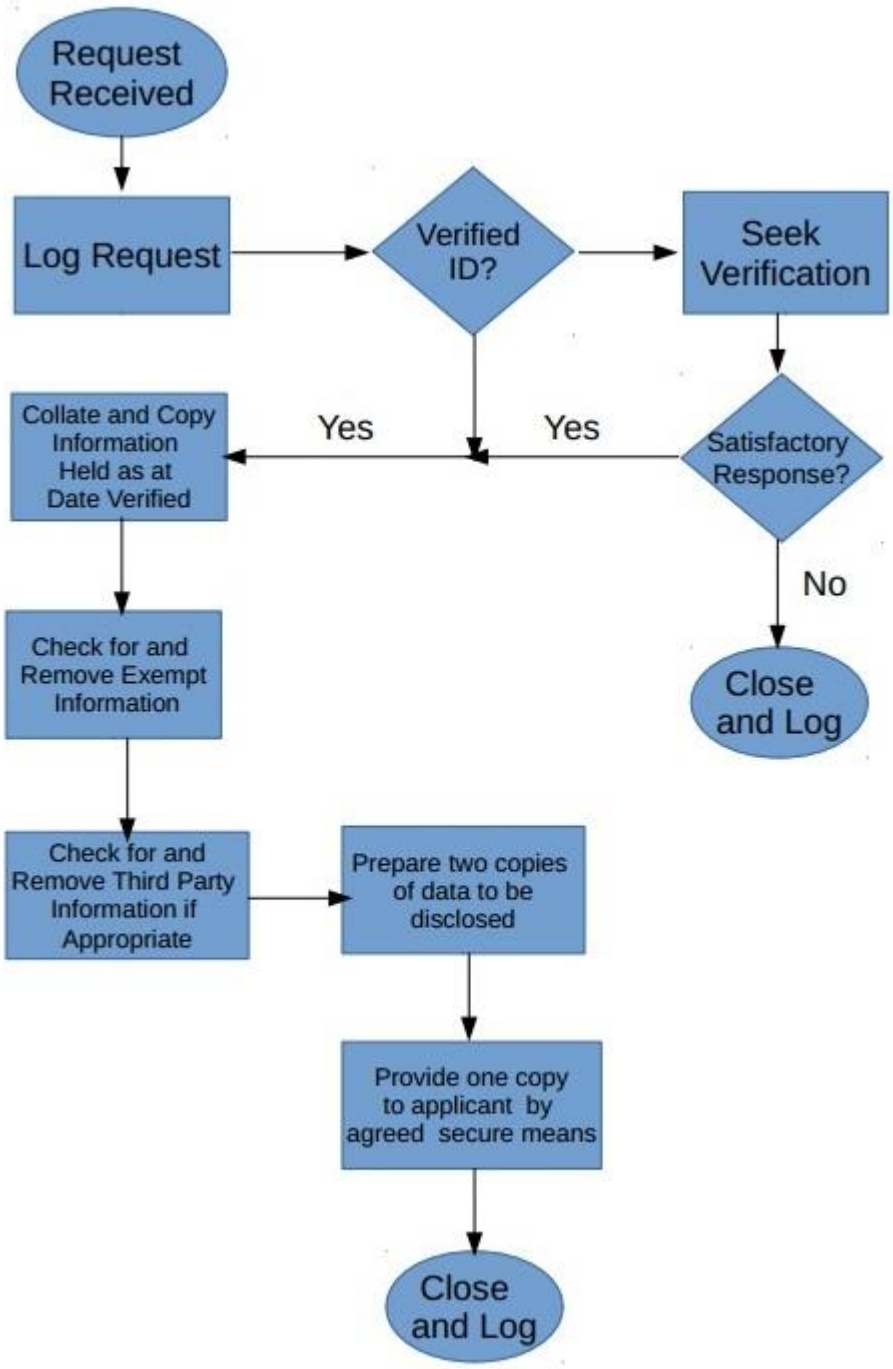
It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a SAR is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Told how long it will be kept;
- Told of their rights, such as rectification, erasure, objecting to or restriction of processing;
- Told of their right to complain to the Information Commissioner;
- Told about any automated decision making or profiling using the data;
- Told about safeguards in place if the data is sent outside the European Union;
- Given a copy of the information comprising the data; and given available details of the source of the data (if it was not them).

No fee is payable in most cases. This would only be possible if the request was manifestly excessive.

A response must be given promptly and in any event within one month. This may be extended to a maximum of three months on grounds of complexity. For further information see Trust Subject Access Guidance.

Processing a Subject Access Request



Stage one – receipt of request

Simple and routine requests for information, which happens to be personal data, need not be treated as an SAR if they can be categorised as “Business as Usual” (BAU) – see guidance for more details.

Requests do not need to be in writing. They normally will be and if anyone seeks to make a formal SAR orally they should receive a written response setting out the Trust’s advice or intentions relating to the request. Requests may be included in other correspondence. All

requests received which are not being handled as BAU must be directed immediately to:

- The Patient Support and Complaints Team PSCT@uhbristol.nhs.uk for requests related to complaints;
- To Workforce & Organisational Development EmployeeServices@UHBristol.nhs.uk if the request is from an employee or ex-employee for access to employment records;
- Information Governance at Trust Headquarters InformationGovernance@UHBristol.nhs.uk in any other case.

Requests initially received by the wrong team must be forwarded immediately to the correct team.

Once received all requests must be managed by a case manager who has had SAR training and is familiar with the Trust SAR Guidance requirements. Administrative tasks such as requesting departments to provide information, copying, updating the case register and preparing (but not sending other than routine updates) correspondence may be delegated. Upon receipt the request must be logged in the appropriate SAR register including the date of receipt and a case manager must be allocated.

The requester's identity must be validated. The case manager must be reasonably satisfied of the identity. Typically this will be by provision of two forms of identity with the application such as copies of driving licence, passport or birth certificate in addition to other relevant information confirming the applicant's address e.g. copy of a utility bill. A less stringent test may be appropriate e.g. for a current employee using a Trust email address. A more stringent test may be applied if there are any suspicions about identity. The validation date will be entered in the SAR register and may therefore be the same or later than the date received. The time limit for responses runs from the validation date.

If the request has been validated the case manager will send the applicant a letter of acknowledgement (see appendix 1.1) or if it is considered to be a complex case e.g. a staff disciplinary with large amounts of information to be assessed use letter appendix 1.2.

In many cases the best approach to verifying identity is to have a dialogue with the applicant. By exchanging information from the files (some of which at least will need to be retrieved) which only the applicant is likely to know the Trust can have reasonable confidence in the identification. A sample script will be found at appendix 1.3 which may be adapted to the specific case.

Where the request is submitted on behalf of another person validation includes verifying that the other person is authorised to act – see SAR Guidance.

See SAR guidance or seek advice from the data protection officer (DPO) in cases of uncertainty over validation issues.

If identity cannot be verified use and adapt letter in appendix 1.4 to advise the applicant.

If at any stage, for any reason, it appears that a full response will not be delivered within 1 month or any previous time estimate given to the applicant the case manager must ensure that the applicant is advised of:

- The delay;
- The reason for the delay;
- A current time estimate for a full response;
- If the delay is for operational or resource reasons, rather than the complexity of the request, or in any case beyond three months, the applicant's right to complain to the

Information Commissioner.

The applicant must be kept informed of any changes to the time estimate. For example where third party views/consent are being requested this would normally be regarded as complex and an extension should be made to allow reasonable time to consult and to allow the third party to challenge e.g. any decision to override confidentiality.

Stage two – retrieving the information

Requests for copies of required information should be made to the relevant department(s) or record holders(s) and copies of the request should be retained as part of the case file e.g. as a Datix attachment. Responses should be requested to be provided within 7 days and requests followed up promptly in the absence of a full response. See request email appendix 2.1.

If it is unclear what information the Trust may hold, the template letter in appendix 2.2 may be sent. If an individual cannot clarify or simply insists on all information held on them within the organisation, a search of all relevant databases, filing systems and email archives should be initiated.

Types of personal information that might be held by the Trust are:

- Personnel/human resources files if the applicant is/was a member of staff or applied for a post within the organisation. **Note:** personnel records are in multiple locations. There are central paper and electronic records held by Employee Services, Medical HR, or Corporate HR and also operational records kept by line management. See Staff Employment Records Procedures.
- Complaints files.
- Client files or reports such as delayed transfers or applications for funding.
- Payments made or received by the applicant.
- Information from other organisations held by the Trust.
- Information held by Occupational Health. **Note:** although these usually contain medical information, this is not, typically, a health record.

Stage three – reviewing the information

When the available information has been collected, copied and collated it must be carefully reviewed.

Information about other people MUST be removed or redacted if it does not also relate to the applicant. For information which is about another person but also about the applicant (mixed data), an assessment whether to disclose must be made in accordance with Paragraph 14 of Schedule 2 to the Data Protection Act 2018. See SAR Guidance for further details. Such assessments may only be made by a person who has had training in handling SARs.

It may be appropriate to seek consent of the other person to disclose mixed data. Remember this will involve disclosing that the applicant has made a SAR – see SAR Guidance. Typical occasions would be in relation to references received which are marked confidential, or where complaints have been made about a data subject. In many cases complaints cannot be anonymised – the nature and circumstances of the complaint may be sufficient to identify the complainant even if formal identifiers are removed.

If it is appropriate to seek consent see letter appendix 3.1. If consent is given, send an acknowledgment in appendix 3.2. If consent is refused, a decision must be made. The advice of the DPO should be sought when making this decision. The result should be recorded and

notified to the other person as in appendix 3.3. Particularly in contentious cases there should be a suitable gap between this and any disclosure which overrides the refusal of consent to allow the other person to take advice.

Where information is withheld or redacted on this basis the reasons should be explained. As much of the information requested should be given, without disclosing the identity of the third party where possible.

The SAR log must be updated with details of the course of action including the reasoning behind why consent was not sought or considered not appropriate if relevant.

The review must also carefully consider whether any information held, or the fact of any disclosures made is exempt. Again see SAR Guidance for further details. Such assessments may only be made by a person who has had training in handling SARs.

Where any exemptions are applied the reasons should be explained unless to do so would defeat the purpose of the exemption. The SAR log must be updated with details of the course of action including details of any information which is to be withheld, the type of and reasoning behind any exemption applied.

Careful consideration must be given, prior to disclosure, whether the applicant would suffer any harm or distress on receipt of the information. This should be the subject of discussion with the relevant departmental manager. The view of the DPO may be sought. However, unlike with health records, there is no legal basis for withholding the information on such grounds. The purpose is to decide whether access may be mediated e.g. by asking the applicant to come in and discuss the matters of concern.

On conclusion of the review, unless all material has been passed for disclosure, there should be three copies of the records (either paper or electronic):

- The original collated copies;
- A copy marked for redaction/removal;
- A copy with the marked material redacted or removed.

The third copy will go to the applicant in due course. The second copy is retained so that, in the event of a review/complaint it is clear what has been provided to the applicant. The first copy is retained in the event that the review process has to be repeated or revised following a complaint or review request.

Stage four – releasing/refusing the information

As soon as the request has been processed, the information which has been judged to be the applicant's personal data, and is not exempt, should be released using the applicant's preferred method i.e. sent via mail, email, collection or viewing. Standard response letters should be used and adapted as necessary (see appendixes 4.1 – 4.4).

The choice is that of the applicant but the applicant must be advised of any risks relating to his choice. Responses sent by email containing personal data must use the [secure] option. Responses sent using a CD as medium must be encrypted and the password sent separately.

If the information is to be sent by post to the applicant, the information must be sent by special delivery annotated 'Private and Confidential', 'Addressee only' and packaged securely. The special delivery reference number should be logged.

If the applicant has chosen to collect the information from the relevant Trust office, then a receipt

will be required to be signed and photographic ID (e.g. passport or driving licence) must be provided to confirm the recipient's identity. An agent may collect if he/she has signed authority and can produce the applicant's ID information.

If the applicant has chosen, and the Trust has agreed to allow the information to be viewed, a member of the Information Governance (IG)/Human Resources (HR) team will write to the applicant to arrange a convenient time and place that is both suitable to the Trust and the applicant within the time limit or any notified extension.

The viewing should be of photocopied information. Any copies required by the applicant at viewing should be marked and copied at a convenient time. The applicant should not simply be given the viewed copy as that is the Trust's record of what was viewed.

If, exceptionally, there is no other choice but to view the original record, the process must be witnessed by a member of the IG /HR team who must ensure that the applicant is not left alone with the records at any time.

Up to a maximum of one hour will normally be allowed for the applicant to spend viewing the information. However this time may be extended, if justified, with the IG/HR team member's discretion. The applicant will be informed of the time allowance prior to and as a condition of the viewing.

In all instances the applicant should be informed of their rights to complain both to the DPO and to the ICO.

Following release of the information, copies of the documentation should be stored manually in accordance with Records Management Procedures. The date of release and file reference should then be logged.

If the application has been denied, restricted, or no information has been found, the applicant should be notified in writing using the standard letters (see appendixes 4.1 – 4.4). There is no requirement to explain the reason for denying or restricting the information but in accordance with the SAR guidance this should be done where possible.

All decisions must be recorded with reasons.

Complaints or Requests for Internal Review

Complaints or requests for review should be submitted within two months of the date of receipt of the final response. They should be forwarded, as should any complaint received throughout the process, to:

Data Protection Officer, University Hospitals Bristol NHS Foundation Trust, Trust Headquarters, Marlborough Street, Bristol, BS1 3NU. Email: InformationGovernance@UHBristol.nhs.uk

Requestors, who are not content with the outcome of any internal review, have the right to apply directly to the Information Commissioner for a decision under Article 77.

RELATED DOCUMENTS

Subject Access Guidance Non-Health Records
http://nww.avon.nhs.uk/dms/download.aspx?did=21920
Data Protection Policy
http://nww.avon.nhs.uk/dms/download.aspx?did=21609
Information Governance Policy
http://nww.avon.nhs.uk/dms/download.aspx?did=11662

AUTHORISING BODY Information Risk Management Group

QUERIES Contact Data Protection Officer at Trust Headquarters.
InformationGovernance@UHBristol.nhs.uk

Appendixes

Stage One - Receipt of request

1.1 Acknowledgement of request - standard
1.2 Acknowledgement of request – complex case
1.3 Script - Verifying the identity of a data subject
1.4 Unable to verify identity

Stage Two - Processing of request

2.1 Internal email asking staff to search their records
2.2 Clarifying a subject access request (further information required)

Stage Three - Reviewing the information

3.1 Obtaining the opinions of a third party (including referees)
3.2 Acknowledgment of the third party's consent to disclose the information
3.3 Acknowledgment of the consideration of the third party's opinions regarding disclosure of the information and explanation of the decision reached

Stage Four - Releasing/refusing the information

4.1 Replying to a subject access request providing the requested information in full or where information has been withheld but no explanation is being given
4.2 Release of part of the information, when the remainder is covered by an explained exemption
4.3 Information not Held
4.4 Replying to a follow up where applicant specifies specific information which was omitted, without explanation, from a previous response

1.1 Acknowledgement - standard

[Name] [Address]

[Date]

Dear [Name]

Thank you for your [letter/email/fax] of [date] requesting information about [subject]. I am writing to let you know that we have received your request and will process it as soon as possible, and this should be within one month of [insert validation date].

If for any reason we are unable to complete the request by that date we will let you know before that date.

You will find further details about your rights in relation to your information on the Trust's website

at: http://www.uhbristol.nhs.uk/privacy

You will also find general information about your rights on the Information Commissioner's website at: https://ico.org.uk/your-data-matters/

Yours sincerely

1.2 Acknowledgement – complex case

[Name] [Address]

[Date]

Dear [Name]

Thank you for your [letter/email/fax] of [date] requesting information about [subject]. I am writing to let you know that we have received your request and will process it as soon as possible. Normally we would deal with such requests within a maximum of one month of [insert validation date]. However in this case the request is complex because [insert short explanation]. It may therefore take a little longer than a month and in such cases the law allows us up to three months from that date. Our current estimate is that we should complete the request by [date].

If for any reason we are unable to complete the request by that date we will let you know before that date.

You will find further details about your rights in relation to your information on the Trust's website at: http://www.uhbristol.nhs.uk/privacy

You will also find general information about your rights on the Information Commissioner's website at: https://ico.org.uk/your-data-matters/

Yours sincerely

1.3 Script - Verifying the identity of a data subject

A script for a telephone call to confirm the identity of an individual making a subject access request.

Good morning [name of data subject]

I am telephoning from the University Hospitals Bristol NHS Trust about the request you have made for access to your personal data. My name is [your name] and I am dealing with your request.

Before we can go further, I have to confirm your identity. This is to make sure that we do not release your data to anyone other than yourself. Please could I ask you two questions, based on the information that we hold about you, to confirm your identity?

The first question is: [question 1]

The second question is: [question 2]

[If the person answers the questions correctly:]

Thank you for answering these questions correctly. I will note on our file that I have confirmed

your identity, and we will now deal with your request.

[If the person refused to answer the question:]

I am sorry, we cannot comply with your request until we have confirmed your identity. If you are not prepared to answer the questions, is there another way we could confirm your identity?

[If the person answers the question incorrectly:]

I am sorry, you answered question [1/2] incorrectly. Is there another way we could confirm your identity?

[Please make a record of the telephone conversation outcome.]

1.4 Unable to verify identity

[Name] [Address]

[Date]

Dear [Name]

RE: Subject Access Request

I refer to our recent telephone conversation/exchange of correspondence about your request for access to personal information the Trust may hold about you.

I regret that we have been unable to satisfactorily confirm your identity because [explain].

This means we are not able to provide a full response to your request. Where the Trust holds personal data about an individual the Trust must comply with the data protection principles set out in the General Data Protection Regulations 2016(GDPR). The information is also likely to be confidential and disclosing personal information to the wrong person would be a breach of the principles and the law of confidentiality. Article 12.6 of GDPR allows us, where we have reasonable doubts concerning the identity of a person making a request, to request the provision of additional information necessary to confirm the identity of the requester, and until that information is provided we are not required to comply with the request.

You will find further details about your rights in relation to your information on the Trust's website at: http://www.uhbristol.nhs.uk/privacy

You will also find general information about your rights on the Information Commissioner's website at: https://ico.org.uk/your-data-matters/

I would again invite you to take the following steps to confirm your identity: [set out requirements].

Until you do so I must also give you formal notice that the Trust, as a public authority, is unable to confirm or deny whether it holds the information you have requested as doing so would itself reveal personal information. In such cases s40(5)(a) of the Freedom of Information Act 2000 says that the duty to confirm or deny holding personal data does not arise.

Alternatively you have the right to make a formal complaint to the Trust's Data Protection Officer if you are not happy with this response. The contact details are:

Data Protection Officer

University Hospitals Bristol NHS Foundation Trust
Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR if you think the Trust is infringing your rights in this matter. The contact details are below. You will also find further information about your rights generally and making a valid Subject Access Request on the ICO website at: https://ico.org.uk/your-data-matters/.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

Yours sincerely

2.1 Internal email asking staff to search their records

Subject: Data Protection Act: Subject access request

Dear [Name]

The Trust has received a subject access request for the following information [details of requested information] relating to [identify individual – full name/DOB/Address/NHS Number (if relevant)/Staff Number (if relevant) etc.].

Please search your [paper records/e-mails/computer drives] and locate any relevant information.

The Trust has a statutory deadline for responding to this request. Please return all relevant information to [name] within 7 days of [date] along with a record of how long it has taken you to retrieve it. If for any reason it you are unable to do this within 7 days please let us know immediately with a full explanation of the difficulty.

Yours sincerely

2.2 Clarifying a subject access request (further information required)

[Name] [Address]

[Date]

Dear [Name]

Thank you for your letter of [date] making a subject access request for [whatever information has been requested].

So that we can process your request we need some more information to identify the information you are requesting. The Trust has over 9,000 staff spread over a large number of departments and locations. You will not have had any dealings with most of these staff and departments. It is

difficult to answer an enquiry that asks for all information the Trust holds on you, as this is too general a request for us to be able to locate the information you want. Information that will help us answer your request includes the type of information in which you are interested (for example: recent medical records), and the areas of the Trust you believe may hold relevant information. Any further information you can supply will assist us in answering your request.

We intend to instruct the following areas to search but further information is needed if this does not cover everything:

• [List areas which will be searched]

I look forward to receiving clarification to help us identify the information you are requesting.

Yours sincerely

3.1 Obtaining the opinions of a third party (including referees)

[Name] [Address]

[Date]

Dear [Name of third party]

We have received a request from [name of data subject (the applicant) under the General Data Protection Regulation under which the applicant has a right to receive copies of the personal information we hold about [him/her] unless particular exemptions apply. These exemptions may include, where we cannot disclose the information without also disclosing information about someone else, particularly where we may owe a duty of confidentiality to that other person.

In our search we identified some information about the applicant that involves you, so I am writing to seek your views on the disclosure of the information described below to the applicant.

We will take your views into account when deciding what we disclose and the applicant may have the right to challenge any non-disclosure decisions that we make.

The items concerned are included in [describe file]. They are:

1. [Itemise the documents concerned or for large quantities list the number of pages]

[I enclose copies of [describe] for you information. *NB It may not be appropriate to copy everything only that which relates to the person being written to.*

Please could you let me know whether or not you have any objections to the disclosure to the applicant of your [whatever the document is]/[this information which identifies you]? *Adapt as necessary.*

If you do have any objections, please could you explain their nature so that we can take your views into account when considering whether to disclose?

There are tight time limits in law for our response to the applicant, so I would be grateful if you could reply to my letter by [7 days max]. If we do not here from you we will assume that you object to disclosure.

If you would like clarification of any of the points I have raised, please feel free to contact me.

Yours sincerely

3.2 Acknowledgment of the third party's consent to disclose the information

[Name] [Address]

[Date]

Dear [Name of referee]

[Name of data subject]

Thank you for your letter dated [date] concerning the disclosure of [whatever the document is] in response to [name of data subject's] data subject access request. As you have no objections to the release of the information, I will include it in the information that I supply to [name of data subject] in response to [his/her] subject access request.

Thank you for taking the time to consider this matter.

Yours sincerely

3.3 Acknowledgment of the consideration of the third party's opinions regarding disclosure of the information and explanation of decision reached

[Name] [Address]

[Date]

Dear [Name of referee]

[Name of data subject]

Thank you for your letter dated [date] concerning the disclosure of [whatever the document is] in response to [name of data subject's] subject access request and for taking the time to consider this matter.

Or

We note that you have not responded to our letter of [date] concerning the disclosure of [whatever the document is] in response to [name of data subject's] subject access request.

Following consideration of your views/In view of your lack of response – we are required to consider whether it is reasonable in all the circumstances to disclose the information to the applicant.

We have decided [not to disclose/to disclose] to the applicant the following information which may identify you. [Specify]

[If disclosing despite objections give reasons for your decision and then conclude.]

[We propose to make this disclosure on {date 7 days ahead – NB keep applicant advised of any changes to time scale}. If you wish to challenge this decision you should do so immediately and may contact the Trust's Data Protection Officer. The contact details are:

Data Protection Officer
University Hospitals Bristol NHS Foundation Trust

Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR if you think the Trust is infringing your rights in this matter. The contact details are below.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

Yours sincerely

4.1: Replying to a subject access request providing the requested information in full or where information has been withheld but no explanation is being given

[Name] [Address]

[Date]

Dear [Name of data subject]

Subject Access Request

Thank you for your letter of [date] making a request for [subject]. We have treated this as a request for your personal data held by the Trust under Article 15 of the General Data Protection Regulation 2016 (GDPR).

We are pleased to enclose the information you are entitled to.

We hold this information because [explain briefly the reason we hold the data]

We would normally expect to retain this information for [insert brief details of applicable retention period] {If relevant: This information has been/may be disclosed to [recipient or categories of recipient]}.

{If data was not received from the subject: We received this information from [insert details]

You may have rights under GDPR to ask us to rectify this data if you think it is inaccurate, or to ask that we erase the data or restrict its use. You may also have rights to object to object to some processing activities. You will find further details of these rights and generally about how we handle personal data on the Trust's website at: http://www.uhbristol.nhs.uk/privacy or on the Information Commissioner's website at: https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

If you think we have not fully answered your request you may complain to the Trust's Data Protection Officer. The contact details are:

Data Protection Officer

University Hospitals Bristol NHS Foundation Trust
Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right at any time to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR if you think the Trust has infringed your rights in relation to processing your personal data. The contact details are below.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

[Copyright in the information you have been given belongs to the University Hospitals Bristol NHS Trust or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.] *Note: Only include this in exceptional cases e.g. if the data disclosed includes photographic images which are of commercial value to the Trust – make clear which bits of information it applies to.*

Yours sincerely

4.2: Release of part of the information, when the remainder is covered by an explained exemption

[Name] [Address]

[Date]

Dear [Name of data subject]

Subject Access Request

Thank you for your letter of [date] making a request for [subject]. We have treated this as a request for your personal data held by the Trust under Article 15 of the General Data Protection Regulation 2016 (GDPR).

We are pleased to enclose the information you are entitled to.

We hold this information because [explain briefly the reason we hold the data].

We would normally expect to retain this information for [insert brief details of applicable retention period]. {If relevant: This information has been/may be disclosed to [recipient or categories of recipient]}.

{If data was not received from the subject: We received this information from [insert details]

You may have rights under GDPR to ask us to rectify this data if you think it is inaccurate, or to ask that we erase the data or restrict its use. You may also have rights to object to object to

some processing activities. You will find further details of these rights and generally about how we handle personal data on the Trust's website at: http://www.uhbristol.nhs.uk/privacy or on the Information Commissioner's website at: https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/.

We would advise that we do hold some personal data relating to you which has not been disclosed. You will notice that [if there are redactions] parts of the document(s) have been blacked out and/or that there are some obvious gaps from what you requested.

This is because [explain why it is exempt]. e.g. *there is information about other people which we cannot separate from your own personal data and we have assessed, as required by Paragraph 14 of Schedule 2 to the Data Protection Act 2018, that it would not be reasonable in all the circumstances to disclose this to you.*

Or

It is exempt from the right of access because it is legally privileged.

Or

It is exempt from the right of access because it is a confidential reference given by or on behalf of the Trust.

Or

[insert details of exemption applied].

If you think we have not properly answered your request you may complain to the Trust's Data Protection Officer. The contact details are:

Data Protection Officer
University Hospitals Bristol NHS Foundation Trust
Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right at any time to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR if you think the Trust has infringed your rights in relation to processing your personal data. The contact details are below.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

[Copyright in the information you have been given belongs to the University Hospitals Bristol NHS Trust or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.] *Note: Only include this in exceptional cases e.g. if the data disclosed includes*

photographic images which are of commercial value to the Trust – make clear which bits of information it applies to.

Yours sincerely

4.3: Information not Held

[Name] [Address]

[Date]

Dear [Name of data subject]

Subject Access Request

Thank you for your letter of [date] making a request for [subject]. We have treated this as a request for your personal data held by the Trust under Article 15 of the General Data Protection Regulation 2016 (GDPR).

We regret that following all reasonable searches we are unable to locate any personal data relating to you of that description held by the Trust. That may be because we have already deleted any records we may have held, or you may have been mistaken about which organisation might hold such records.

If you think we have not properly answered your request you may complain to the Trust's Data Protection Officer. The contact details are:

Data Protection Officer
University Hospitals Bristol NHS Foundation Trust
Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right at any time to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR if you think the Trust has infringed your rights in relation to processing your personal data. The contact details are below.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

4.4 Replying to a follow up where applicant specifies specific information which was omitted, without explanation, from a previous response

[Name] [Address]

[Date]

Dear [Name of data subject]

Subject Access Request

Thank you for your letter of [date] in relation to our response, dated [insert date of letter Ref. 4.1 4.2 or 4.3] to your Subject Access Request.

You have now specifically asked for disclosure of the following [additional] information: [describe].

We consider our previous response to be a full and proper response taking into account your rights under Article 15 of the General Data Protection Regulation 2016. We are therefore unable to confirm or deny whether we hold any personal data relating to you of the type you have specified. We are applying section 40(5)(a) of the Freedom of Information Act 2000 which says that the duty to confirm or deny holding information ***does not arise*** in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of section 40(1). Section 40(1) itself provides an absolute exemption for disclosure of information under the Freedom of Information Act which is the personal data of the applicant.

This is because even saying we held such data, if it existed, would be disclosing personal data about you.

We would remind you that, if you think we have not properly answered your request you may complain to the Trust's Data Protection Officer. The contact details are:

Data Protection Officer
University Hospitals Bristol NHS Foundation Trust
Marlborough Street
BRISTOL
BS1 3NU

Email: InformationGovernance@UHBristol.nhs.uk

You also have the right at any time to lodge a formal complaint with the Information Commissioner's Office under Article 77 of the GDPR and section 50 of the Freedom of Information Act 2000 if you think the Trust has infringed your rights in relation to processing your personal data or your request. The contact details are below.

Information Commissioner's Office
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF

Email: casework@ico.org.uk

Yours sincerely