19 February 2024

Information Governance Training 2024 - 2025

Collaboration: IMPERIAL COLLEGE HEALTH PARTNERS

Welcome!

Introductions – Your trainers for today:

Robin, Laura, Mila

What is this training for?

Your annual IG training and to meet NHSE requirements

Why is it important for us to complete this training?

Improving IG awareness and compliance across ICHP

Housekeeping

Things to note before we start…

- Please mute your microphone
- Training will be recorded
- Slides and recording will be shared after the session
- Training assessment afterwards
- Short break halfway through
- Q&A at the end – but feel free to add questions to the comments as we go

Part 1A

What we are going to cover

Part 1A

- Information Governance – An Overview
- Data Protection Definitions
- Identifiable Data vs De-identified Data
- Data Protection Principles
- Lawful Bases for Processing

Information Governance – An Overview

What is Information Governance?

Information governance (**IG**), is the **management** and **overall strategy** of how an organisation **uses information**.

IG balances the **use**, **security** and **risk** of information.

"A set of policies, procedures and technical controls at an organisation which are there to govern access, its use and protect the data"

How does IG help ICHP?

Good IG practices helps with:

A. **Legal compliance** - Data Protection Act 2018, UK GDPR, Common Law Duty of Confidentiality, PECR etc.;

B. **Operational use and transparency** – letting the people whose personal data you are using know how you're are using their data and how you should use their data;

C. **Reduces expenditures associated with legal disclosures** – people wanting access to their data, law firms requiring you to disclose information for legal claims and court orders.

Incorporating IG into ICHP

- ICHP must establish a **consistent** and **logical framework** for anyone who has **access to data** that ICHP is responsible for

- We **must handle that data properly** and we can do this through our **policies**, **procedures** and **technical controls** we have in place.

- Our **policies** are designed to guide proper **behaviour** regarding how the information we process should be handled by users.
- Our **technical controls** dictate the technical **rules** and **restrictions** for users accessing data within systems.

Data Protection Definitions

Data Protection Legislation

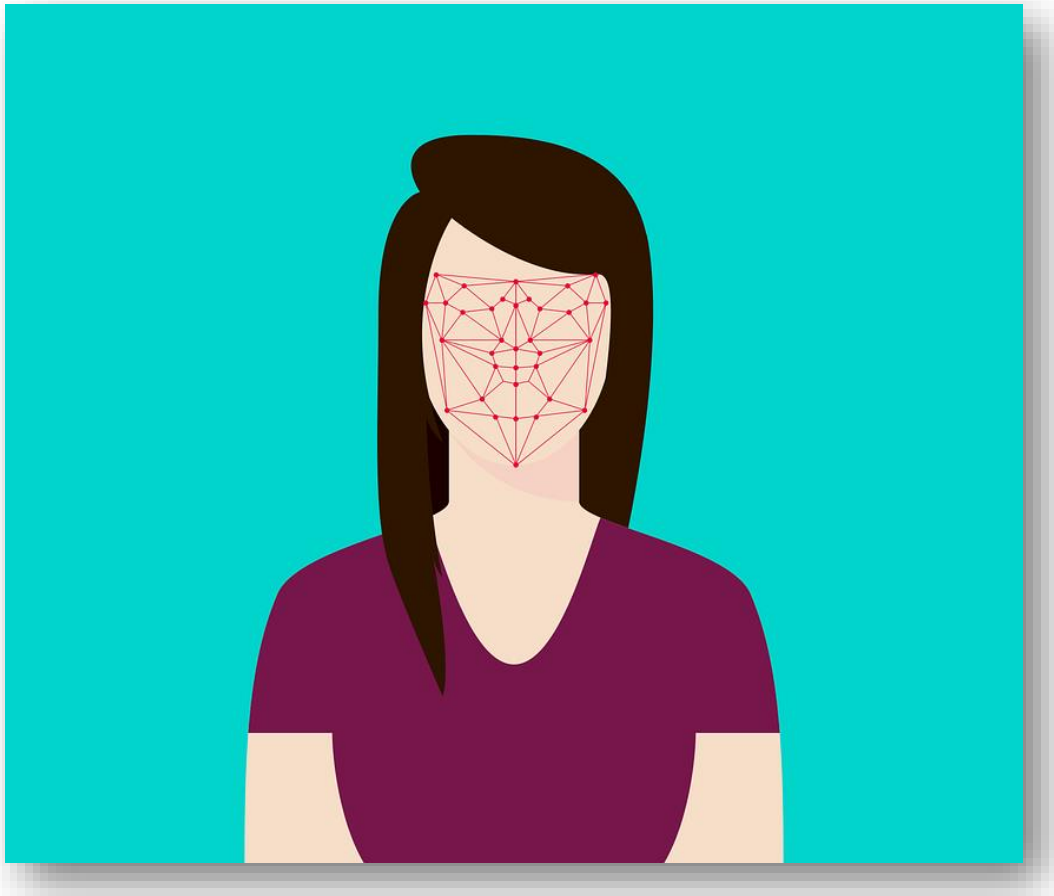
- **UK GDPR / DPA 2018** – the primary legal instruments for data protection in the UK
- **Freedom of Information Act 2000** – access to information held by public bodies
- **Access to Health Records Act 1990** – access to deceased person's health records

Data Protection Definitions - What is Personal Data?

Personal data means any information relating to an **identified** or **identifiable** natural person.

Personal data is a **STRICTLY** defined concept.

"*The principles of data protection should not apply to **anonymous information,** namely information which does not relate to an identified or identifiable natural person*"

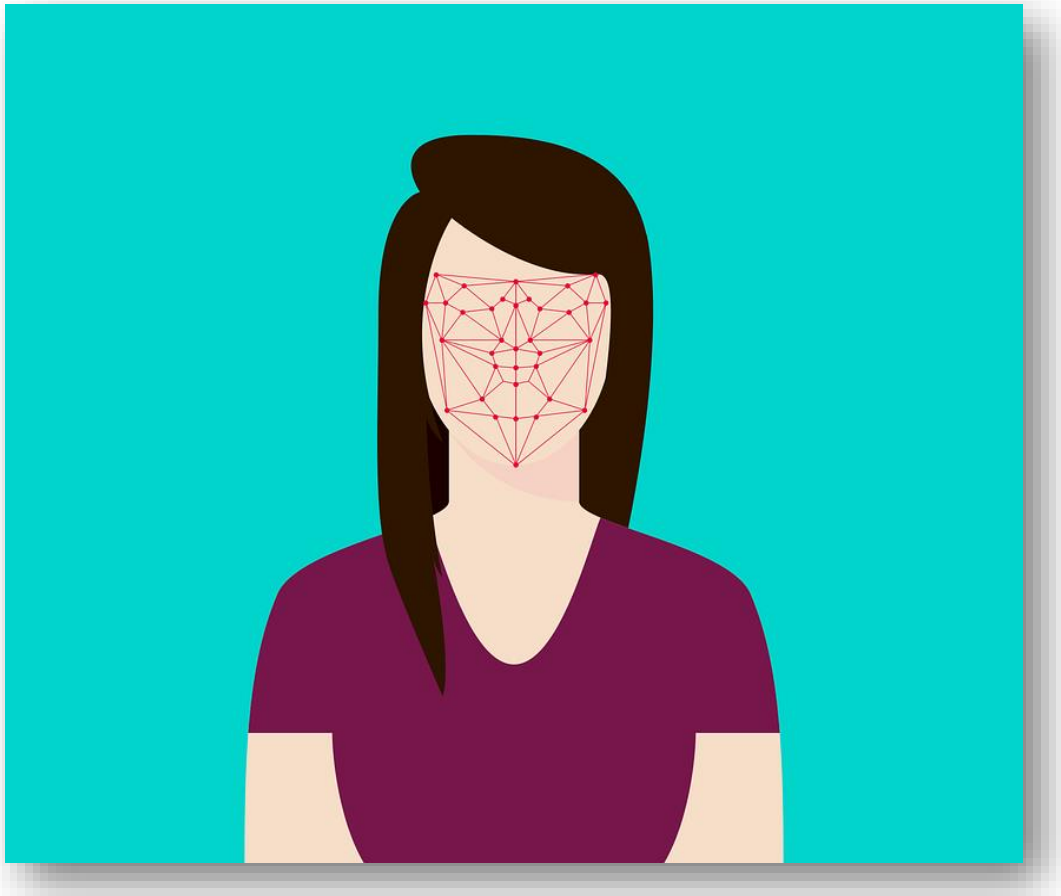


Data Protection Definitions - What is Personal Data?

EXAMPLES INCLUDE:

- A name
- NHS number
- A phone number
- A personal work email address
- A surname
- A nickname

Anything that identifies or could be used to identify an individual!



Data Protection Definitions – What are special categories of personal data?

Article 9(1) UK GDPR provides that data is 'special' when it reveals an individual's:

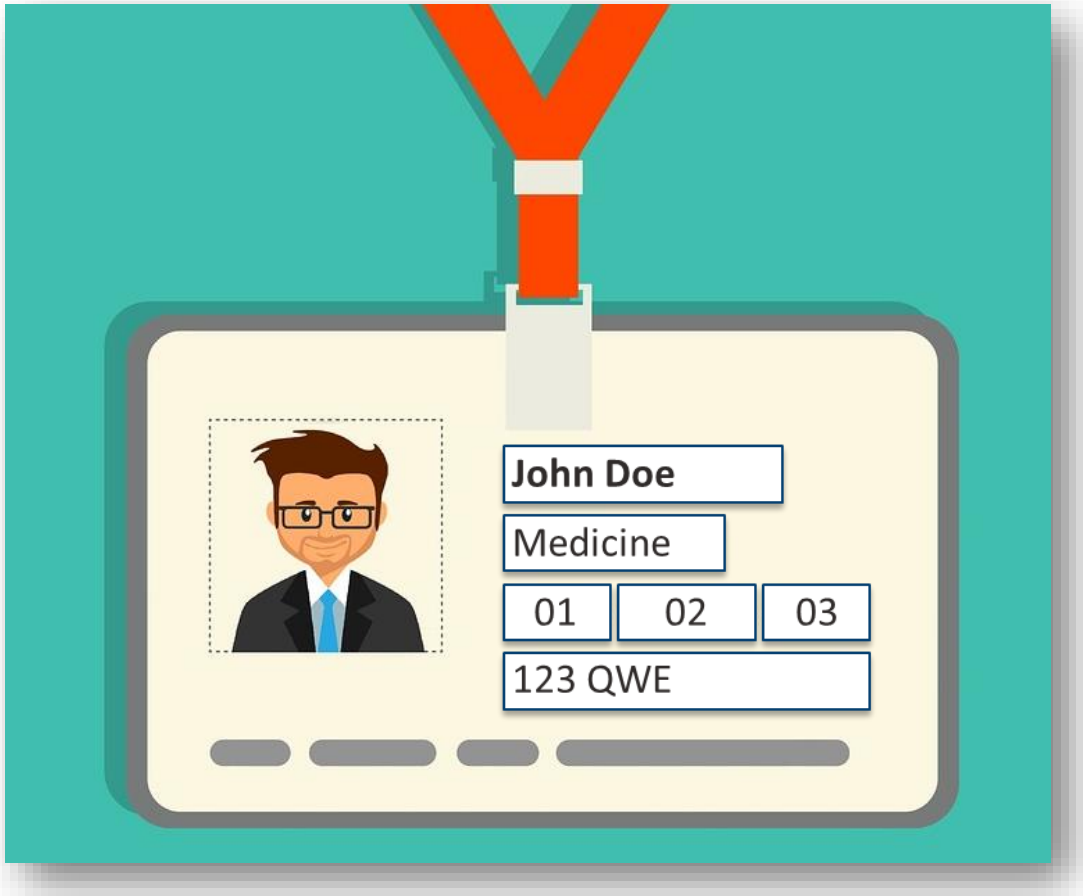
- racial or ethnic origin
- political opinions
- religious or philosophical belief
- trade union membership
- health
- sex life or sexual orientation
- genetic data and biometric data for purpose of identifying an individual

Data Protection Definitions - What is a data subject?

A **data subject** is an identifiable natural person to whom the personal data relates.

Identifiable – a person who can be identified from the personal data

Natural – a living person, not a corporation or someone who is deceased



Data Protection Definitions – What is Processing?

Processing means **any** operation which is performed on personal data

Processing is a **BROADLY** defined concept which includes:

- collection
- recording
- organisation
- structuring
- storage
- alteration
- retrieval
- consultation
- use
- transmission
- dissemination
- combination
- restriction
- erasure
- destruction

Data Protection Definitions – What is a Data Controller?

Data Controller

Means any entity which alone, or jointly with others, determines the **purposes [why]** and **means [how]** of the processing of personal data.

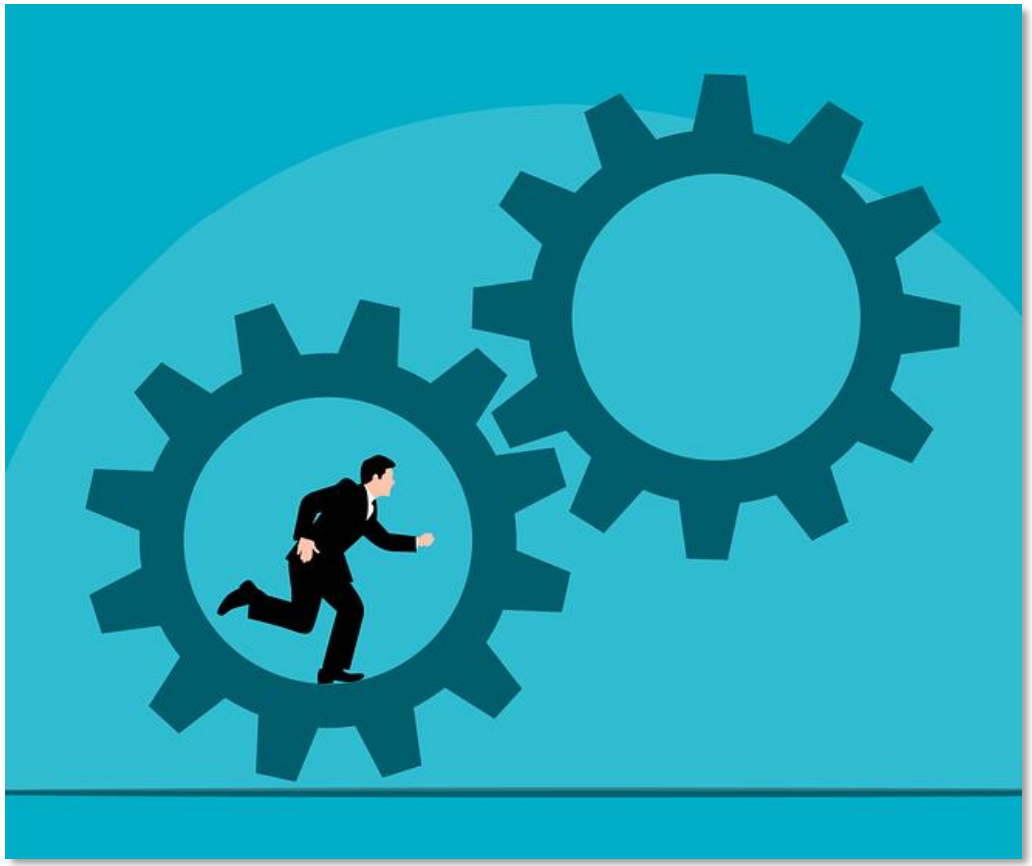
Joint Data Controller

Where two or more controllers jointly determine the purposes and means of processing.

Data Protection Definitions – What is a Data Processor?

Data Processor

Means anyone (both natural and legal) which processes personal data on **behalf** of the data controller.



Data Protection Definitions – What is a Data Controller/Processor? - EXAMPLE

ICHP

NHS Partner

Identifiable vs De-Identified Data

Identifiable Data Vs De-identified Data

Identifiable data - Data which relates directly or indirectly to a living person.

De-identified (pseudonymised) data – Data which could identify a living person, directly or indirectly, **if connected to other data**. Under the UK GDPR, de-identified/pseudonymised data is still considered personal data because re-identification of the data subject is possible when connected to the additional data.

Anonymised data - Data which **cannot be re-identified** by any reasonable means. Anonymised data is not considered personal data and is outside the scope of the UK GDPR.

Pseudonymisation

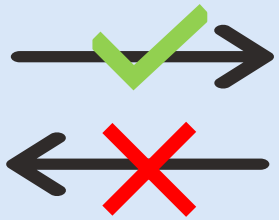
Pseudonymisation - Example

Original Dataset				
Full name	**DOB**	**Phone number**	**Postcode**	**Height**
Anna Mosey	23/03/1999	07654 967765	SW4 7JB	168 cm
Paul Devine	03/04/1987	07809 057654	SE6 4RN	187 cm
Steve Huxley	10/12/1942	07123 873456	N5 1UA	161 cm
Mary Moore	30/09/1992	07998 987654	N18 2TX	180 cm

Pseudonymised Dataset				
Pseudonym 🔑	**Birth year**	**Phone number**	**Postcode**	**Height**
A2Qb9	1999	-	SW4	165 - 170 cm
Y7bP8	1987	-	SE6	185 - 190 cm
9oK7B	1942	-	N5	160 - 165 cm
NB46k	1992	-	N18	180 - 185 cm

Anonymisation

Jane Doe

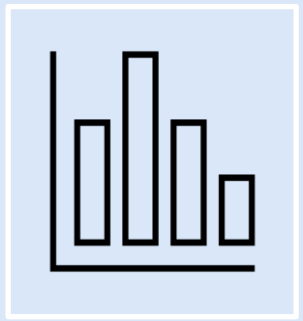


f7e4 8r_

Anonymisation - Example

INDIVIDUAL LEVEL DATA

- Mary, Max and John are gluten intolerant
- Jill has a peanut allergy
- Tom and Sarah are vegetarian
- Lily is vegan



AGGREGATED DATA

- 42.8% are gluten intolerant
- 14.2% have a peanut allergy
- 28.5% are vegetarian
- 14.2% are vegan

Identifiable Data Vs De-identified Data

Health care professionals require **identifiable data** of their patient to deliver healthcare

Secondary purposes can be carried out using **de-identified data, or anonymized data**

Note: Where **identifiable data** is used for secondary purposes, either consent or approval from the Confidentiality Advisory Group is needed.

How/Where Does This Apply To Me?

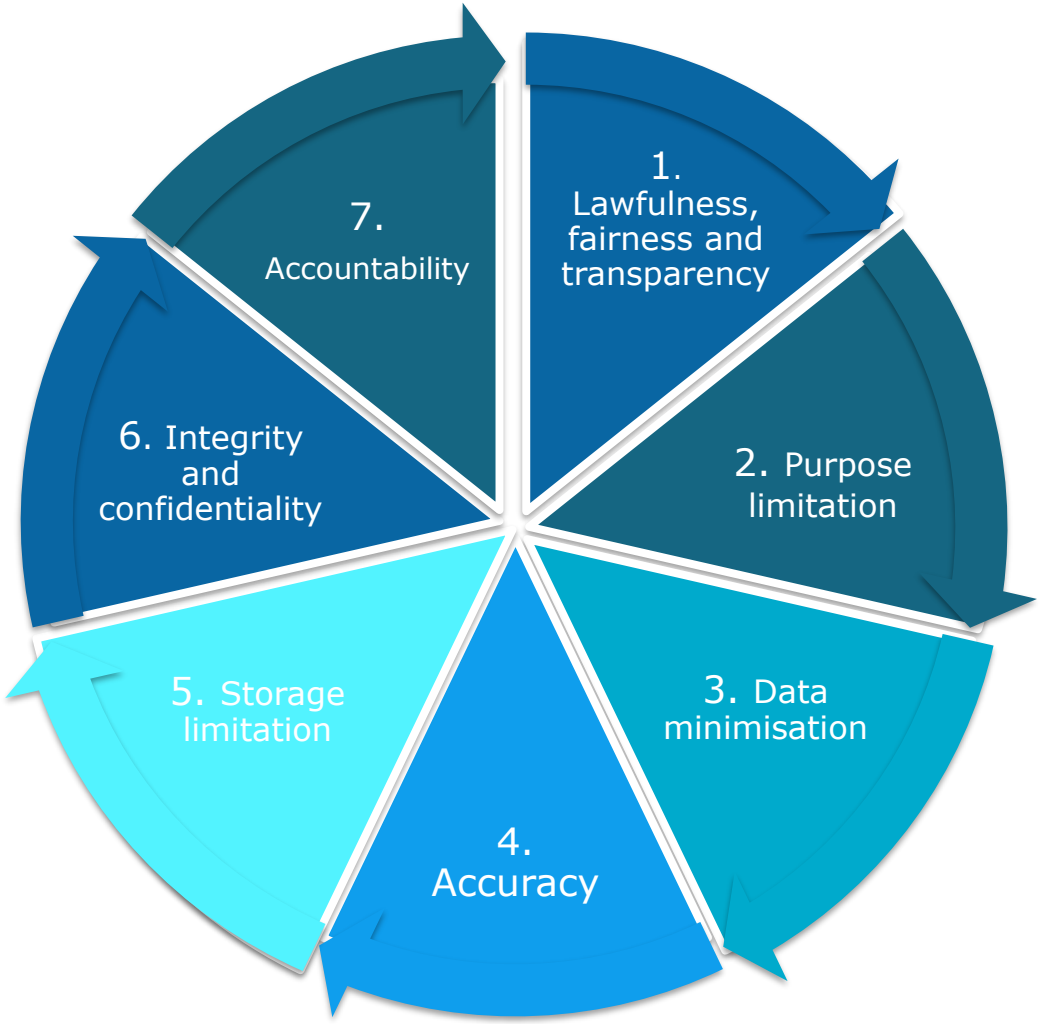
- **ICHP mostly uses de-identified data** from our NHS partners within North West London and beyond to drive innovation. We also sometimes process personal data to undertake projects.
- Whether or not the data is identifiable or de-identified, **we usually receive instructions (by way of a contract) from our NHS partners as to how we should process their personal data**.
- We are entrusted and **contractually obliged to adhere to the wishes of our NHS partners** and cannot lawfully process the data outside of our scope (except in very limited circumstances).

Data Protection Principles

Data Protection Principles

the 'spirit' of the regime

Any given data processing activity must comply with each of these principles.



1. Lawfulness, fairness and transparency

Personal data shall be processed:

Lawfully	Fairly	In a transparent manner
		
• Grounding the processing activity on appropriate lawful bases (covered later in the presentation) • Complying with any applicable legislation	Handling people's data in ways they would reasonably expect, without deceiving or misleading them. Example: if in your Privacy Notice you state that you process personal data for statistical analysis, it would not be fair if you then use that data for marketing purposes	• Being open and honest • Use plain English • Provide information about your **purpose** • Inform what **data categories** you will process

2. Purpose limitation

Personal data shall be collected for **a specific purpose** and not re-used in a manner **incompatible** with that purpose.

What is specific?

- Clearly identify **why** you need to undertake that data processing activity
- Too vague or general goals are not sufficient

Too vague: marketing, improving our services, improving users' experience, security purposes, future research

Specific: medical research

How to check if a new purpose is compatible with the original one?

- What is/is there a link between the original purpose and the new one?
- What is the context in which the data was collected?
- What is the relationship with the data subject?
- How will the new purpose impact the individuals?
- Are appropriate/additional safeguards in place, such as encryption or pseudonymisation?
- What data categories are subjected to the processing?

3. Data minimisation

Personal data shall be **adequate, relevant** and **limited to what is strictly necessary** to achieve the identified purpose.

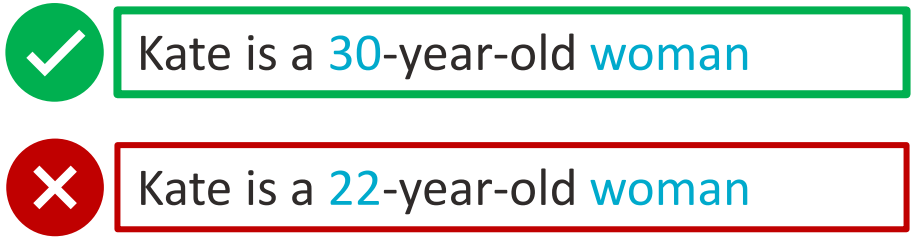
Can you achieve that purpose by not using some categories of personal data?

- **Yes** → You should stop using any unnecessary data
- **No** → You comply with the data minimisation principle
- **Maybe** → **Helpful considerations:**
  a) If your data does not serve the purpose, it is inadequate
  b) Is there a less intrusive way to achieve your purpose?
  c) Can you restrict the data in terms of geography (W5 instead of W5 3JF), demographic (age instead of full date of birth) or clinical factors?
  d) Can you use de-identified data instead of identifiable?

4. Accuracy

Personal data shall be **accurate** and **up-to-date**.

Personal data is accurate when provides a **correct** and **updated** information about the individual it refers to:



How to keep personal data accurate?

- Ensure you review the accuracy of data on a regular basis
- Identify when you need to update it to properly fulfil your purpose
- Update data when necessary

5. Storage limitation

Personal data shall be **not kept for longer than is necessary** for the identified purpose.

- Do not keep data ‘just in case’
- Ensure that you erase or anonymise data you no longer need
- If there is no set retention period data, regularly review whether you still need the data
- Delete from any back-up

Important Note
NHS organisations involved in health and social care must follow the retention schedules set out by legislation and regulations.

NHS England: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

6. Integrity and confidentiality

Personal data shall be processed with appropriate **security measures** to ensure **integrity** and **confidentiality**.

Integrity

Ensuring that data is processed in a secure way

- To prevent data being accidentally or deliberately compromised
- Covers information security and cybersecurity
- But also physical and organisational security measures

Confidentiality

Ensuring that data is treated with confidence

- **Access**/visibility of the data should be **restricted** to people directly involved in the data processing activity
- Whenever possible, data shall be processed in a **de-identified** format

7. Accountability

Organisations shall be able to demonstrate compliance with the entirety of UK GDPR

How?

- Put in place written contracts that set out the parties' responsibilities
- Maintain your Record of Processing Activities
- Review your internal policies and recovery plans
- Have reporting structures and evaluation procedures in place
- Conduct DPIAs when required

Lawful Bases for Processing

Lawful Bases

Article 6(1) states there are 6 lawful bases a data controller can rely on:

A. **Consent** (use only where another does not apply)
B. **Contract** (with a person; e.g. employment)
C. **Legal obligation**
D. **Vital interests** (necessary to protect the life of another)
E. **Task in Public interest or exercising official authority**
F. **Legitimate interests**

Lawful bases

Article 9(2) states there are 10 lawful bases for processing **special category data:**

a) Explicit consent

b) Necessary for employment purposes

c) Necessary to protect somebody's vital interests

d) Legitimate activities of political, religious, charitable bodies

e) Data is already manifestly made public by data subject

f) Necessary for legal reasons

g) Substantial public interest

h) Provision of health and social care systems

i) Necessary in area of public health

j) Necessary for scientific or historical research

<u>Why different lawful bases?</u>

Given the sensitive information revealed by special category of data (religion, sexual orientation, ethnicity, etc.), the UK GDPR requires higher threshold to lawfully process these data categories.

Most relevant lawful bases for ICHP

(**If** and **when** acting as a Data Controller)

For **non-special categories of personal data:**

- **Consent**: Individuals consent to the processing of their personal data when they sign up to receive ICHP's newsletter or marketing mailing list
- **Legitimate interest**: to deal with an enquiry or complaint submitted via the 'contact us' section of the website
- **Performance of a task carried out in the public interest:** where ICHP performs a task related to public health and the management of health care services

For **special categories of personal data:**

- **Explicit consent**: If individuals' health data or employee's ethnicity for internal diversity statistics, explicit consent will be sought
- **Employment, social security and social protection**: When ICHP is processing special category of personal data of its employees, it does so to fulfil its obligations under employment and social security laws.
- **Necessary for scientific or historical research:** where ICHP performs a task related to a public interest in the area of public health and the management of health care services

End of Part 1A

Part 1B

What we are going to cover

Part 1B

- Data Protection by Design & Default
- Data Protection Impact Assessments (DPIAS)
- Personal Data Breaches
- Data Subject Rights
- Freedom of Information (FOI) Requests

Data Protection by ‘Design’ and by ‘Default’

Privacy by Design

What is privacy by design?

UK GDPR requires organisations to have appropriate technical and organisational measures to implement in its approach to protecting the rights and freedoms of individuals and the processing of their personal data.

Implementing privacy by design

ICHP should consider privacy and data at the outset of new projects. You can assist this by getting IGS team involved at the earliest opportunity.

Benefits of privacy by design

This will mean less risk in the future, and not having to change projects down the line when it is realised a certain aspect of the project is not lawful.

Privacy by Default

Implementing privacy by default

UK GDPR requires organisations to only process the data that is necessary to achieve their specific purpose.

Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose.

It does not require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

You might want to consider:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.

Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessment

What is a DPIA?

A DPIA is a comprehensive assessment of a project which processes personal data in order to ascertain the impact of the processing and any associated risks which result from it.

- Demonstrates compliance and accountability
- Must be done ***before*** processing starts
- ***Is not*** an obstacle to processing, but ensures it is done safely in line with data protection legislation
- Necessary where processing of personal data is likely to be **'high risk'**

Examples of ‘high risk’

Are the following examples ‘high risk’?

A hospital processing patients’ health data via its information system	✓	Health data and processing on a large scale
Gathering of public social media data for generating profiles about individuals and targeting them for your services	✓	Data matching and profiling
Sending a digest to a mailing list of subscribers	✗	Not high risk

Data Protection Impact Assessment

What do I need to know?

If you are starting a project where you believe a DPIA might be necessary, contact IGS for assistance and support on the next steps.

You are not expected to complete this alone and there is a team who can help you with the assessment.

- Be proactive. Start the assessment in the early stages of a project.
- Engage with IG and be open to implementing any suggested changes to make the project more secure with data protection regulations.

Personal Data Breaches

Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful:

- Alteration;
- Unauthorised disclosure;
- Access;
- Loss; or
- Destruction of personal data.

You must report any personal data breach or suspected security incidents **immediately** to IGS by following the appropriate process.

With 72 hours

IMPERIAL COLLEGE HEALTH PARTNERS

1. Personal data breach is identified or suspected

2. You fill out section 2 and 3 of the **Incident Report Form** and send to IGS

3. We will fill out remaining sections of the **Incident Report Form** and carry out risk assessment

Your Responsibility

4a. We will advise you on risk mitigation steps (i.e., recalling email incorrectly sent)

4b. We shall notify the ICO, and the affected individual where necessary

IGS **Responsibility**

Data Subject Rights

Data Subject Rights

The UK GDPR provides data subjects with the following rights:

- The Right to be **Informed** in clear and concise manner about how their data is used by the organisation involved in any data processing activity;
- The Right of **Access** and receive a copy of their personal data, and other supplementary information;
- The Right to **Rectification,** to have inaccurate personal data rectified, or completed if it is incomplete;
- The Right to **Erasure** also known as the right to be forgotten – meaning that you are supposed to delete individual's personal data upon their request;
- The Right to **Restriction of Processing** if the accuracy of data is contested, the processing is unlawful, the data subject has objected to the processing and the controller no longer needs the data to pursue the purpose;
- The Right to **Data Portability** the right to receive a copy of their personal data or to have their personal data transmitted from one controller to another controller;
- The Right to **Object** to processing in certain circumstances, noting that individuals have the absolute right to object to the processing if it is for direct marketing purposes;
- The Right to **not be subject to Automated Decision-Making** data subjects can refuse to be subject of decisions made without any human involvement.

Important takeaways for ICHP

- Although your DPO may be the first point of contact for data subjects, individuals may contact anyone part of your organisation.
- These requests can come in any form - onus is on all staff to recognise and action request
- Organisations must respond within 1 month in most cases
- Poor awareness can lead to increased IG complaints and ICO involvement

It is important all staff know of these rights and what to do; you must have policies and procedures, so that you can allow individuals to exercise their rights easily

Freedom of Information (FOI) Requests

Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) regulates access to information held by the public authorities.

Principle

People, members of the public, have a right to know about the activities of public authorities, unless there is a good reason for them not to.

↗ **Public authorities** must:

1)Publish certain information proactively - (https://ico.org.uk/for-organisations/guide-to-freedom-of-information/);

2)Respond to request of information within 20 working days.

↗Every **member of the public**, individuals or organisations, have the right to make a freedom of information request.

Data Subject Rights and FOI requests

The FOIA provides an exemption that interplay with the protection granted by the UK GDPR

If the information contains personal data and disclosing it would breach one of the data protection principles, you should not disclose the information.

Case by Case

Considerations:

A) Whether the info contains personal data

B) Whether the disclosure would breach art. 5 of the UK GDPR

C) Does ICHP have a legal basis to release the information?

D) Is disclosing the information fair?

End of Part 1B

5 minute break - Please take this opportunity to grab yourself a drink or take a short break before we begin again.

Part 2

What are we going to cover?

PART 2

- Marketing
- Information Security and establishing good governance
- Phishing

Marketing

Marketing

Marketing - A subset of engagement which is **"The communication (by whatever means) of advertising or marketing material which is directed to particular individuals."**

What is marketing?

Communication

- Email or text messages
- Phone calls
- Post
- Online behavioral advertising
- Social media marketing

Advertising or marketing material

- Commercial marketing of products and services
- Promotion of aims and ideals such as fundraising, political campaigning, or corporate initiatives that promote community or charitable work

Directed to particular individuals

- Personally addressed post
- Calls to a particular telephone number
- Emails sent to a particular email account
- Online advertising that is targeted to a particular user
- Advertising on social media that is targeted to a particular person

Marketing and the Law

PECR

The Privacy and Electronic Communications Regulations

- Applies to marketing through **electronic means**
- PECR applies even when **no personal data is being processed** (e.g., if you do not know the name of the person you are contacting)
- PECR's rules mainly apply to **unsolicited** marketing messages
  - **Solicited:** a message which is actively requested
  - **Unsolicited:** a message which has not been specifically requested

The UK GDPR

The UK General Data Protection Regulation

- UK GDPR applies **when processing personal data**
- You must have a **lawful basis to process personal data** under UK GDPR.
  - Most likely **consent** or **legitimate interests**

Electronic mail marketing

Consent

- You must not send electronic mail marketing to individuals unless they have **specifically consented** to electronic mail from you.
- **Requirements:**
  - **Knowingly** and **freely given** along with being **clear** and **specific** (same as UK GDPR)
  - Must provide an **accessible way to withdraw consent**

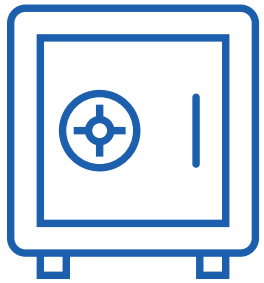
OR

Soft opt-in

- **Soft Opt-In:** rule about existing customers. If an individual has bought from you recently, gave their details and not opted out – they are probably happy to receive marketing messages about similar products or services
- **Must give a chance to opt-out** in every message sent
- Means you can email **existing customers but not to prospective customers**

Information Security and establishing good governance

Information Security



What is it?

- Practice of protecting information by mitigating information risks
  - covers **tools** and **processes** that organisations use to protect information.
- **Includes policies and procedures** that support the broader **technical measures** in place to protect data.
  - ICHP maintains its own policies and procedures which you should follow

Covered in today's training:

- Access Controls
- Appropriate use of Equipment
- Password practices
- Appropriate use of Email
- Record Management

Access Controls

All key systems within ICHP, or systems ICHP staff may have access to, have controls to restrict access, including:

- **Multi-factor authentication** (e.g. two-part authentication)
- **Authorisation process for access to the system** (user registration and deregistration)
- **Assignment of responsibilities for the system** (access, maintain and issue resolution)
- **Login controls** (threshold of failed logins)
- **Audit logs for use of system** (understanding when specific users have accessed the system)
- **Virtual Desktop Infrastructure (VDI)** (digital bubble for secure environments)

Appropriate Use of Equipment

- Only devices **authorised** by ICHP, should be used to transport personal data – this includes any portable devices which should always be encrypted;
- Equipment must be used in an appropriate and professional manner;
- Staff must follow appropriate protocols and procedures;
- Staff responsible for equipment issued to them and for return of equipment no longer required;
- Please see ICHP's **Security Policy, Bring Your Own Device Policy** and **Acceptable Use Policy** for further details on staff responsibilities.

Password Practices

You must **never share your password** with anyone, not even your line manager or any senior staff member;

If you believe your password has been **compromised**, then **change your password immediately**;

Do not use the same password for multiple applications.

Avoid writing down your password on paper or on notes in your computer

Email – Appropriate Use

DO'S

- Double check all recipients email addresses are correct
- Double check any attachments before sending
- Use BCC where sending emails to recipients who do not need to see each other's identity or details
- Send confidential/sensitive information securely by a secure email method
- Remove personal information from emails and use initials where appropriate
- Remove people off an email chain if they no longer need to see the information.

DO NOT'S

- Forward unknown attachments
- Forward long email threads unless you are sure that everything is relevant to the recipient
- Open emails from suspicious email addresses

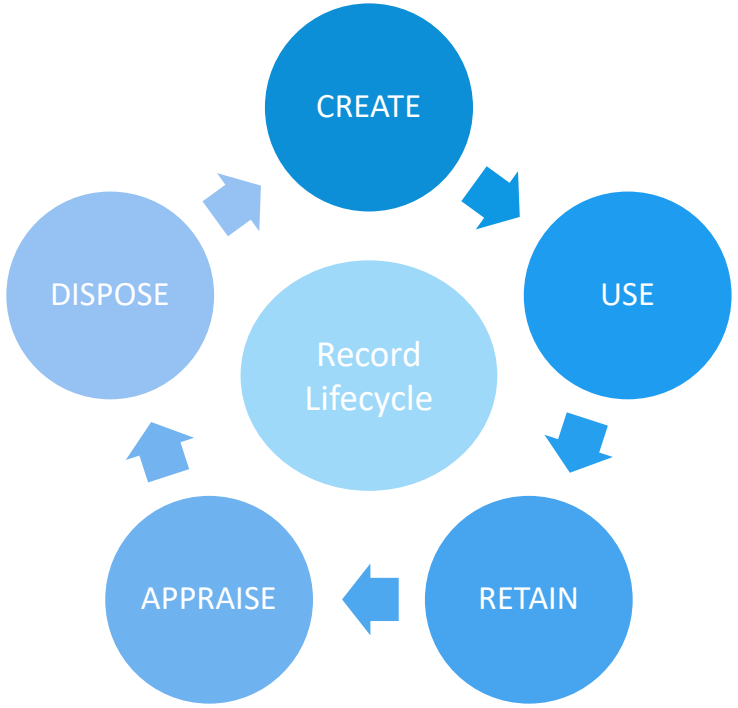
Record Management

Follow ICHP's policies

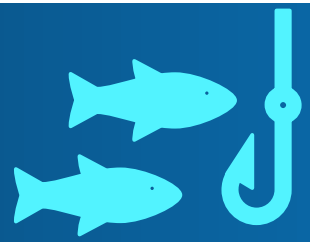
e.g., Information Governance Policy, Information Security Policy, Clear Desk Policy

All staff have a responsibility to:

- Create records in line with ICHP's guidelines
- Save records in the right places
- Use records appropriately (version controls/avoid duplication)
- File records correctly for security and accessibility (right of access)
- Ensure secure disposal/preservation by proper means



Phishing



Phishing

What is it?

Phishing is when criminals use scam emails, text messages or phone calls to trick their victims. It often starts with tricking users into doing 'the *wrong thing',* such as clicking a bad link that will download malware or direct them to a dodgy website for further attacks.

Various forms

Can be text messages, social media, or by phone. Most common to happen over email as it can have a huge and wide reach with a relatively low amount of effort for the attacker.

Chain of events

Phishing can have a snowball effect. If there is a successful attack, it could lead to a series of targeted campaigns in which the messages are even more persuasive and realistic. This is known as ***'spear phishing'***.

Phishing – What to look out for?

Scammers try to quickly gain your trust and aim to pressure you into acting without thinking.

Authority

Criminals often pretend to be important people or organisations to trick you doing what they want.

They could pretend to be senior ICHP staff and directors, Doctors, Solicitors, Government Departments

Urgency

Often the message indicates a limited time to respond to incite panic and acting without thinking. The consequences threatened can be fines or other consequences.

Emotion

Criminals use emotive and often threatening language to disarm the reader, aiming to make you feel panicked, feared, hopeful or curious.

Scarcity

Many phishing messages offer something in short supply such as concert tickets or money. Fear of missing out on good deals or opportunities can make you respond quickly.

Phishing – What to look out for?

Tell-tale signs

- **Sender:** Does the name sound legitimate? Does the email address match the name?
- **Subject line:** Is it alarmist or have excessive punctuation?
- **Logo/branding:** Does it have the correct logo/branding or is it low quality?
- **Unfamiliar/generic greeting:** Look out for generic names, greetings or unusual salutations
- **Inconsistencies:** Look out for inconsistencies amongst email addresses, links, domain names
- **The body:** The messages often have bad grammar, spelling errors, and unusual word choices
- **Hyperlink/ attachment:** Does it look genuine? If you mouseover the link, does it go to the same place?
- **Signature block:** Is it generic or a copy?
- **Requesting sensitive information:** May request login credentials, payment information or sensitive data.

National Cyber Security Centre
a part of GCHQ

Multi-layered phishing mitigations

The following real-world example shows how implementing **layers** of defences can help organisations (in this case a financial sector company of around 4,000 staff) defend themselves against phishing attacks. Reliance on any **single** layer would have missed some of the attacks, and cleaning infecting devices is costly and prohibitively time consuming.

1,800 malicious emails sent to the company in this campaign.

1,800

1,750 emails were stopped by an email filtering service that identified that malware was present.

1,750

50 emails reached user inboxes.

50

36 emails were ignored or reported by staff, using a button in their email client.

25 were reported in total, including some after having been clicked on.

This was the first indication that the attack had got through the initial layer of defences.

36

14 emails were clicked on, launching malware.

14

13 malware installations were unsuccessful because a patching regime had ensured that nearly all devices were up-to-date.

13

1 instance of malware installed.

1

The malware's call home to its operator was detected, reported and blocked. 1 device was seized, investigated and cleaned within a few hours.

How was the organisation attacked?

A financial sector company of around 4,000 employees received 1,800 emails which contained a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.

CPNI
Centre for the Protection of National Infrastructure

How To Report

If you have received a suspicious looking email, or have reasonable doubts about the legitimacy of the email, you should err on the side of caution and follow this process:

1. Do **not open** any **attachments** or **click on any links** or **engage** with any response to the sender.
2. Raise **a ticket** with **Cloud Direct** with the subject line "suspicious email". Attach suspicious email to the ticket.
3. After which, Cloud Direct will then take appropriate action.

Part 3

What are we going to cover?

PART 3

- What are my Responsibilities?
- Key Data Protection Roles in ICHP
- Utilising your IG Service
- Why is IG important? Final takeaways
- Questions & Answers

What are my legal responsibilities?

What are my legal responsibilities?

- You are **contractually required** to adhere to ICHP's suite of Information Governance policies and procedures
- You are required by **statute** to use the personal data properly
- You can **personally** be held criminally liable if you misuse the data.

Contractual/ Professional Responsibilities

- **Misusing** the personal data can amount to gross misconduct under your Contract of Employment
- Can result in triggering **disciplinary procedures**
- If serious/gross misconduct, it would be up to Human Resources to decide whether it would merit **terminating** your contract altogether
- Misusing data can cause professional consequences and being **de-registered** from your professional body

Responsibility under the DPA

Section 170 of the Data Protection Act 2018:

170(1) It is an offence for a person to **knowingly** or **recklessly**:

- To obtain or **disclose** personal data without the **consent** of the controller
- To procure the disclosure of personal data **to another person** without the **consent** of the data controller
- After obtaining personal data, to **retain** it without the **consent** of the person who was the data controller in relation to personal data when it was obtained

Responsibility under the DPA

Section 171 of the Data Protection Act 2018:

171(1) – it is an offence for a person knowingly or recklessly re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data

Key Data Protection Roles in ICHP

Key Data Protection Roles in ICHP

Senior Information Risk Owner (SIRO) – **Axel Heitmueller**

Caldicott Guardian – **Natalie Angus**

Data Protection Officer (DPO) - **Taj Sallamuddin (IGS)**

IT Security Manager – **Cloud Direct**

Information Governance Services (IGS) – **External IG support team**

Utilising your IG Service

Utilising your IG service

*Do you have a **query** regarding data protection or IG?*
*Are you starting a **new project** which involves handling personal data?*

We, IGS, are your external IG support provider, so get in touch with us directly! We are here to help!

Don't ignore IG, don't suffer alone – get in touch:
ichp@informationgovernanceservices.com

Why is IG important? Final takeaways

Why is IG important? Final takeaways

€ 1.2 billion fine for Meta for unlawfully transferring users' data to the US

€ 746 million fine for Amazon for processing user data without a lawful basis

According to Art. 83(4) and (5) of the UK GDPR, ICHP could be fined:

- Up to **£8.7 million** for **less serious** infringements of data protection obligations
- Up to **£17.5 million** for **more serious** data protection violations

Any Questions?

Thank you!

For more questions about this session, please contact us at:

ichp@informationgovernanceservices.com