



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

BMHP6026_BIRM

Week 3

Information Governance and Ethical use of Data

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

www.uwtsd.ac.uk

During the Session...

**Introduction to
information
governance.**

Overview of UK GDPR

**Introduction to ethical
use of patient data**





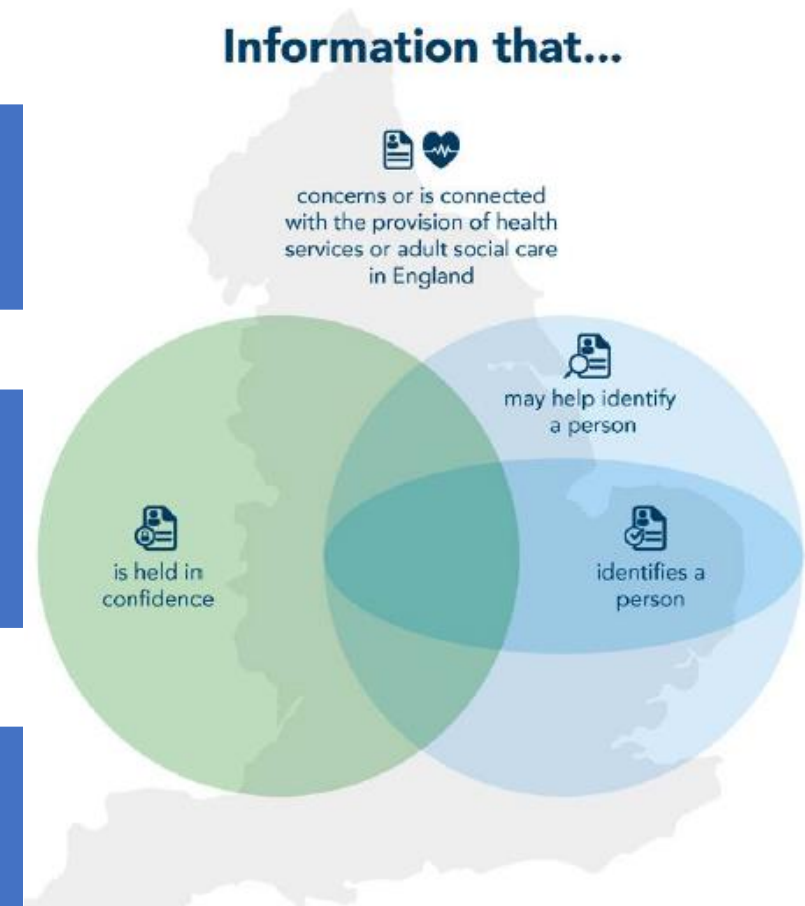
Information Governance

Any organisation that collects, analyses, publishes or disseminates confidential health and care information must follow the Data Protection Act 2018 and UK GDPR.

The Information Commissioner's Office (ICO) clearly defines the steps that organisations must, should and may take to ensure that confidential information is handled appropriately.

Information governance refers to the practice of handling the information of service users, staff and other identifiable individuals.

Information that...



Key Organisations in Information Governance

Information Commissioner's Office (ICO) - national regulator, provides guidance and can issue fines.

NHS England - sets policies and standards for IG across health and care, including digital records.

Department of Health and Social Care (DHSC) - creates legislation and overarching frameworks.

Care Quality Commission (CQC) - checks that health and social care providers meet IG standards as part of inspections.

Local Authorities and Care Providers - responsible for ensuring IG policies are followed at organisational level.

Data Protection and UK GDPR (General Data Protection Regulation)

The Data Protection Act 2018 is a central piece of UK legislation governing the use of personal data, this act incorporates the principles of UK GDPR.

What is Personal Data?

“Any information relating to an identified or identifiable living person (the data subject)” ICO 2023

What is UK GDPR?

““The GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).” Data Protection Act 2018, section 3:10



The UK GDPR sets out Seven Key Principles:

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

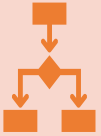
4. Accuracy

5. Storage limitation

6. Integrity and confidentiality (security)

7. Accountability

Why are the Principles Important?



The principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation and inform everything that follows. They do not give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.



Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the UK GDPR.



Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.



The Information Commissioners Office -



The ICO exists to empower people and organisations in the UK through information.

Lawfulness, Fairness and Transparency



(ICO, 2025b)



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Lawfulness and Fairness



An organisation must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data.



An organisation must ensure that you do not do anything with the data in breach of any other laws.

An organisation must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

(ICO, 2025b)

Transparency



An organisation must be clear, open and honest with people from the start about how they will use their personal data.



Purpose Limitation



An organisation must be clear about what their purposes for processing are from the start.



An organisation needs to record their purposes as part of their documentation obligations and specify them in their privacy information for individuals.



An organisation can only use the personal data for a new purpose if either this is compatible with the original purpose, they get consent, or they have a clear obligation or function set out in law.

Discussion Scenario

- A large care organisation has four respite centres and six residential care homes. They plan to open a new over-55's supported living village in Jan 2025.
- The next-of-kin contact data from their internal records system is used to create a marketing mailing list. Emails and postal marketing materials are sent out to the full list of contacts. Details of the open day event are sent twice via sms text message to the listed mobile numbers.

Do you think this is ok?

Why **is** it ok? Or Why **isn't** it ok?





Data Minimisation

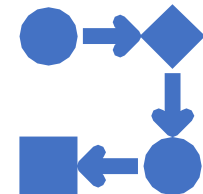
An organisation must ensure the personal data they are processing is:



Adequate - sufficient to properly fulfil the stated purpose;



Relevant - has a rational link to that purpose



Limited to what is necessary - An organisation does not hold more than they need for that purpose.

Example - Data Minimisation

- An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident.
- The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.
- If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work.



Accuracy

An organisation should take all reasonable steps to ensure the personal data they hold is not incorrect or misleading as to any matter of fact.

An organisation may need to keep the personal data updated, although this will depend on what they are using it for.

If an organisation discover that personal data is incorrect or misleading, they must take reasonable steps to correct or erase it as soon as possible.

An organisation must carefully consider any challenges to the accuracy of personal data

Example - Accuracy

A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.

This is technically allowable but can be potentially confusing if not clearly explained.

- *Should records of mistakes always be kept?*
- *How can organisations avoid confusing or misleading people in these cases?*





Storage Limitation

An organisation must not keep personal data for longer than they need it.

An organisation need to think about - and be able to justify - how long they keep personal data. This will depend on your purposes for holding the data.

An organisation needs a policy setting standard retention periods wherever possible, to comply with documentation requirements.

An organisation should also periodically review the data they hold, and erase or anonymise it when they no longer need it.

An organisation must carefully consider any challenges to their retention of data. Individuals have a right to erasure if you no longer need the data.

An organisation can keep personal data for longer if they are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Practical Examples - Storage Limitation

- **Job Applications:** An organisation receives 200 applications for one vacancy. After the post is filled, the applications of unsuccessful candidates should not be kept indefinitely. They can be deleted after a set retention period (e.g. 6 months), unless there is a clear legal reason to keep them.
- **CCTV Footage:** A supermarket might keep CCTV footage for 30 days to monitor incidents. After that time, unless there has been an incident that requires the footage, it should be deleted.
- **Employee Records:** When an employee leaves a job, the employer may need to retain some records (e.g. pension details, tax records), but should delete unnecessary information such as emergency contact details.
- **Customer Data:** A gym keeps contact details of members while their membership is active. Once the membership ends, the data should not be kept indefinitely “just in case,” unless there is a valid reason (e.g. ongoing payment disputes).
- **Research Data:** Universities may keep anonymised research data for many years if it is being stored for scientific or historical purposes, but personal identifiers should be removed where possible.

Integrity and Confidentiality (security)



Consider risk analysis, organisational policies, and physical and technical measures.

Take into account additional requirements about the security of processing - and these also apply to data processors.

Measures must ensure the 'confidentiality, integrity and availability' of systems and services and the personal data processed within them

The measures must also enable organisations to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

Ensure that appropriate processes in place to test the effectiveness of measures, and undertake any required improvements.

A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' -

This is the '**security principle**'.

(IOC, no datea)



Example - Security Breach

In the case of Gloucester City Council, a December 2021 ransomware attack via a phishing email received from a legitimate third-party address, which resulted in personal information being extracted and encrypted.

The ICO investigation found that the Council failed to prevent log tampering, did not have a centralised logging system, or a security information and event management system, in place. That meant the Council could not effectively monitor and respond to security incidents, detect suspicious activities, or identify potential threats.

The ICO also found that the Council **did not recover access to personal information in a timely manner** and was unable to determine if specific groups of people were at risk as a result of the incident.



Gloucester City Council Ransomware attack- 2021



Accountability

The accountability principle requires an organisation to take responsibility for what they do with personal data and how they comply with the other principles.

- **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

A controller must have appropriate measures and records in place to be able to demonstrate compliance.

Example - Accountability

- A hospital uses an automated system in its waiting room to notify patients when to proceed to a consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information.
- The **hospital** will be the **controller** for the personal data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.



UK GDPR - Seven Principles:

Aim to remember the seven key principles of UK GDPR sets :

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality (security)

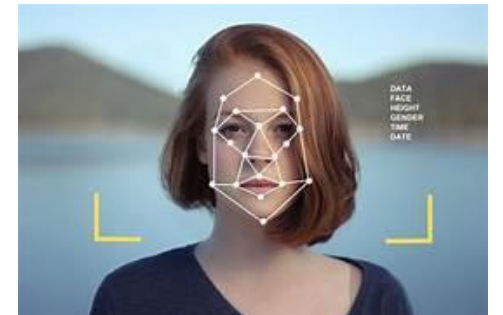
7. Accountability

Video Surveillance and Bio-metrics

Body Worn Video (BWV) - This term describes the use of a video recording or streaming device that has been attached to the clothing of a person.

Facial Recognition Technology (FRT) - This refers to technology that uses mathematics to scan a person's face and make comparisons to stored data in order to determine or verify the identity of a person.

Biometric data - means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR.





Discussion Scenario

An ambulance service wishes for staff to use a BWV system, so that staff can capture any abusive behaviour towards them when they are on duty.

- How could this use of BWV benefit the ambulance staff?
- How could this use of BWV benefit the community?
- What data protections need to be considered?

Discuss in small groups and be prepared to feed-back to the class

Discussion Scenario

An education authority is considering whether to use Facial Recognition Technology (FRT) to verify pupils' identities at the cash register during lunch, in order to deduct money from an online account and facilitate cashless catering.

- How could this use of FRT benefit the individual students?
- How could this use of FRT benefit the community?
- What data protections need to be considered?

Discuss in small groups and be prepared to feed-back to the class



How is NHS Patient Data used in the UK?

Our NHS is unique. In England it looks after 55 million people, from the time we are born until the end of our lives.

The information in our health and care records can be put together to create a set of data that is unmatched anywhere else in the world. It's not about anyone's individual data, but about the data of millions of us as a population.

This data, from across the whole population, is used to monitor and improve care, and it's one of the great strengths of our health service.

But we all know that our health and care information is sensitive, and needs to be kept safe.

This is why NHS Digital exists, created to collect and look after this important information and enable it to be used safely, to improve health and care now, and for future generations.

(NHS Digital, no dateb)



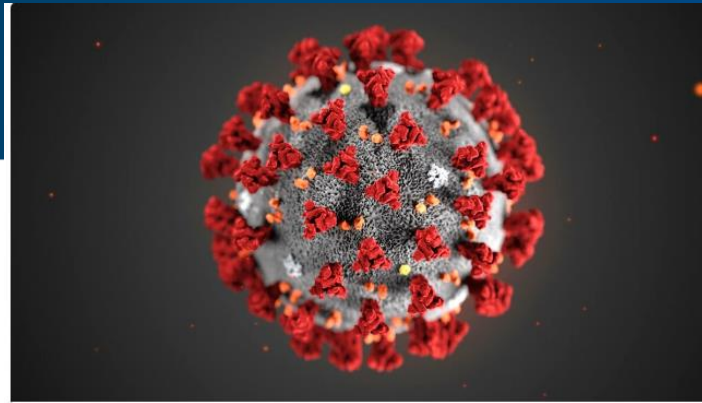
NHS Digital





Deciding on the best care

When medical staff have good data on the care patients receive and how well it works, they can recommend the best care for every individual patient.



Managing contagious diseases

When there is an outbreak of an infectious disease, such as flu, emergency planning committees and the NHS use our data to track its spread and take measures to protect the public, to prevent epidemics.



Planning services, for now and for the future

When we know how many people have a condition, and what their care needs are over time, data can be used to plan which services they will need in the future, making sure services keep up with what the population will need.



Improving efficiency and saving money

Data on health and care across the system can show us where money can be saved by using resources better and becoming more efficient. This means more of the NHS budget can be spent where it's needed most.



Researching and improving treatments

When researchers have access to high quality data on treatments and their success rates, they can use it to research new cures and improve medicines.



Addressing health inequalities

When local authorities and government have good data that covers the whole population, they can identify areas that have worse health outcomes and target health and care resources towards the patients that need them most.

NHS Digital - Key Functions

- Keeps patient data safe and makes sure it is used legally.
- Runs IT systems linking health and care records (e.g. NHS Spine, Summary Care Record).
- Provides digital services like the NHS App, website, e-Referrals and e-Prescriptions.
- Uses data to improve care for all:
 - Monitors NHS performance
 - Manages disease outbreaks
 - Plans future services
 - Supports health research



Digital

Services Data Cyber Developer News About

NHS Digital > Data > Publications > Primary Care Dementia Data > Primary Care Dementia Data, August 2024

Publication, Part of [Primary Care Dementia Data](#)

Primary Care Dementia Data, August 2024

Official statistics

Publication Date:	19 Sep 2024
Geographic Coverage:	England
Geographical	GP practices, Sub-Integrated Care Boards, Integrated Care Boards, Regions, Country, Local Authorities, Government
Granularity:	Office Regions
Date Range:	01 Aug 2023 to 31 Aug 2024

Key Facts

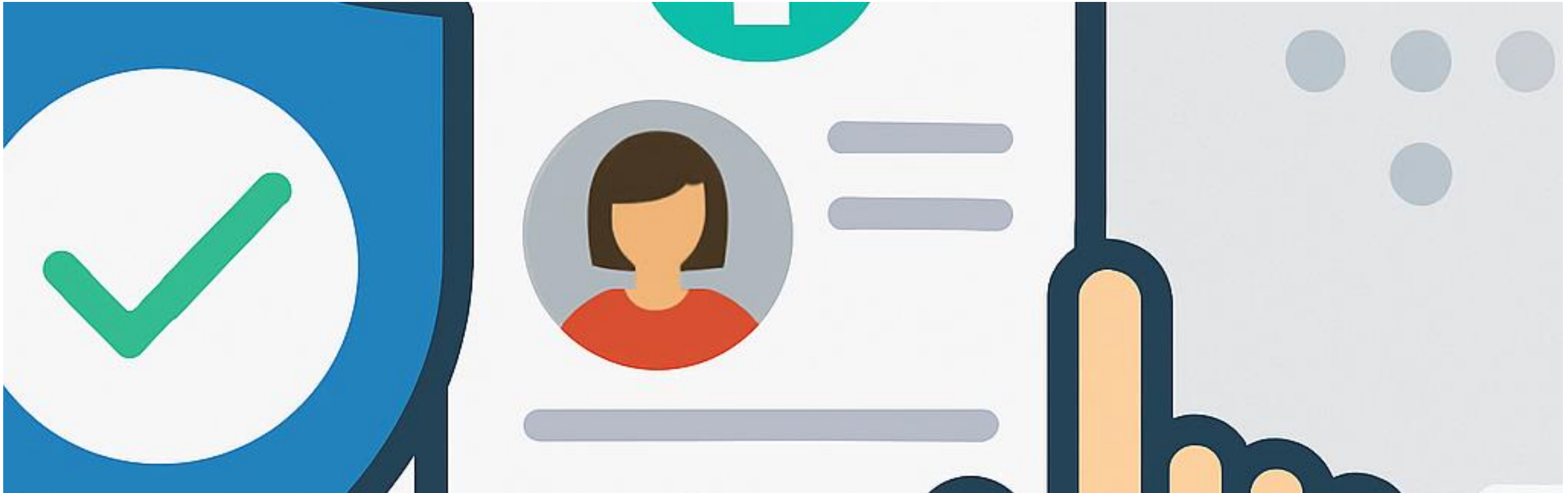


Recorded dementia diagnosis
492,901 patients had a recorded diagnosis of dementia on 31 August 2024, an increase of 2,738 patients since 31 July 2024.

In August 2024, NHS Digital used patient data to develop an overview of Dementia care in Primary care services.

- In what ways do you think that this type of data collection benefits **patients**?
- In what ways do you think this type of data benefits **staff in the workforce**?
- In what way might this data lead to benefits for **local communities**?

Ethical Use of Patient Data



Ethical Use of Patient Data

The National Data Guardian advises the health and adult social care system in England to help ensure that people's confidential information is kept safe and used properly.



Vision

The NDG's vision is for improved health and care outcomes through the safe, appropriate, and ethical use of people's health and social care information.



Mission

- The NDG's mission is to help preserve trust in the confidentiality of our health and social care services. If people are to support the collection and use of their health and care data, they need to be confident that information about their care will remain private and only be used in ways which benefit the public.
- To support the development and maintenance of trustworthy systems and practices, the NDG provides advice, encouragement, and challenge to the health and social care system on the safe, appropriate, and ethical use of people's confidential health and care information.



Objectives

- Four long-term strategic objectives support the NDG's mission:
 - Safeguard trust in the confidentiality of our health and social care system
 - Encourage safe and appropriate information sharing for individual care
 - Support understanding and engagement about how and why data is used
 - Encourage the safe, appropriate, and ethical use of data in system planning, research and innovation that benefits the public.

The Caldicott Principles



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

Principle 2: Use confidential information only when it is necessary

Principle 3: Use the minimum necessary confidential information

Principle 4: Access to confidential information should be on a strict need-to-know basis

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Principle 6: Comply with the law

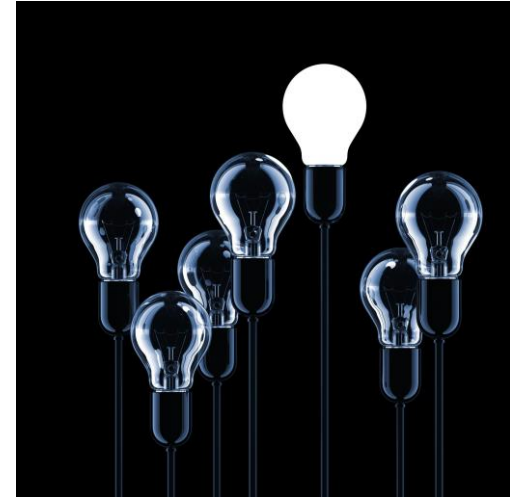
Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Principle 8: Inform patients and service users about how their confidential information is used



Spotlight Innovation

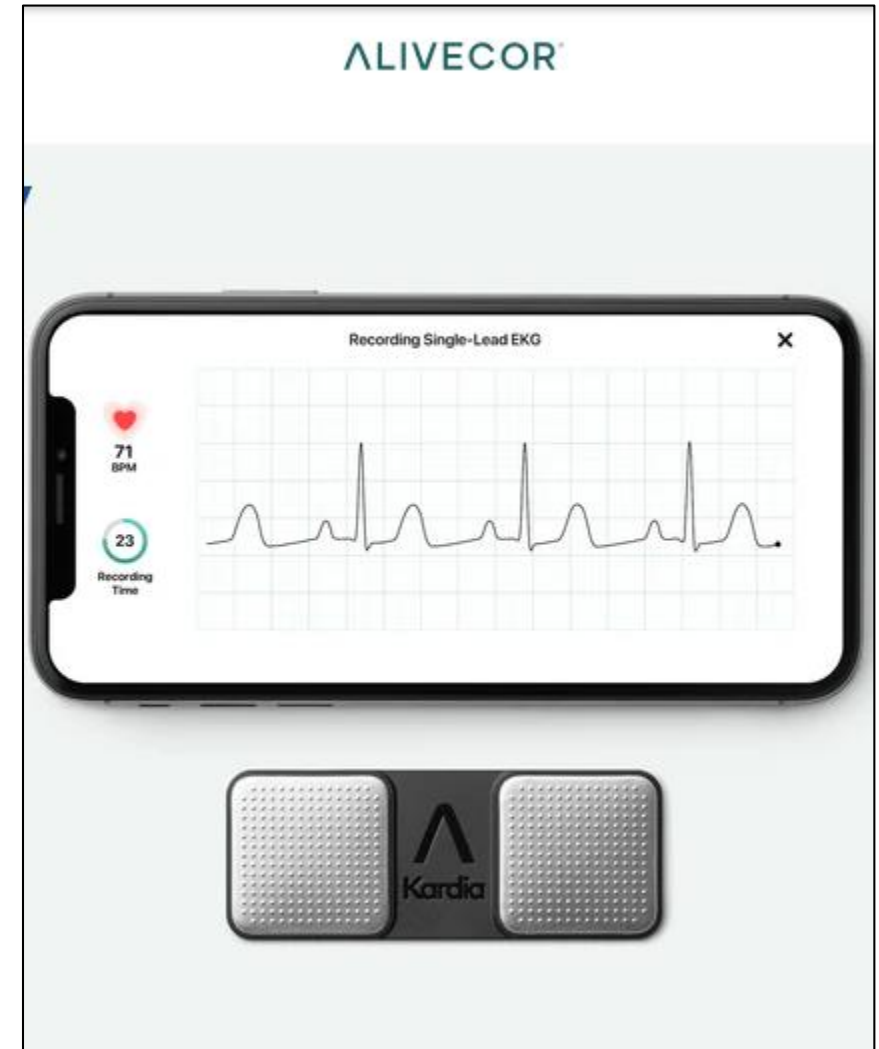
KardiaMobile ...





KardiaMobile - by AliveCor

- **Description:** KardiaMobile is a portable ECG device that allows users to perform heart rhythm checks and detect atrial fibrillation and other arrhythmias. It connects to a smartphone app to provide instant results.
- **Impact:** This technology enables users to monitor their heart health easily and regularly, providing valuable data for early diagnosis and management of heart conditions. It is particularly useful for people with known heart issues or those at risk.





KardiaMobile - by AliveCor

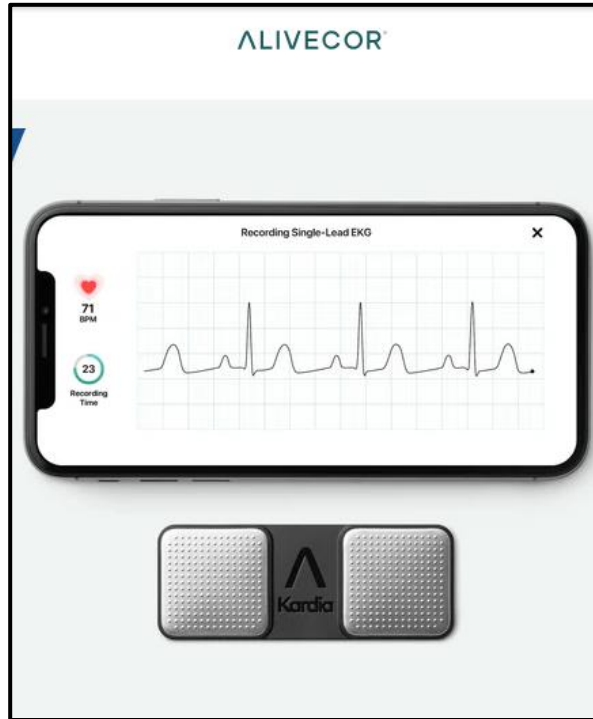




KardiaMobile - by AliveCor



KardiaMobile by AliveCor



These wearable technologies not only help individuals manage their health and fitness but also offer valuable data that can be used by healthcare providers to tailor treatments and interventions.

The integration of such technologies into daily life is contributing to improved health outcomes and more personalised care in the UK.

- How could this type of technology benefit an **individual** with day-to-day life and care?
- How could this type of technology benefit the **workforce**? Or local **communities**?
- What **challenges** could there be with regards to the collection, storage and sharing of this information?

(AliveCor, 2024)



During this session we have...

**Introduced
information
governance.**

**Overviewed Data
Protection and GDPR
in the UK**

**Introduced the Ethical
use of patient data**

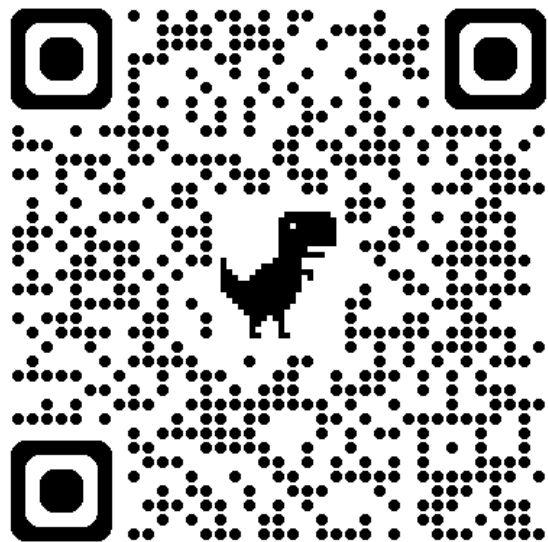
Reference List

- GOV.UK (no date) *NDG About Us* Available at: [About us - National Data Guardian - GOV.UK](#) (Accessed: 11 September 2025).
- ICO (2025d) *Guide to accountability and governance* Available at: [Guide to accountability and governance | ICO](#) (Accessed: 11 September 2025).
- ICO (2025c) *Accuracy* Available at: Principle (a): [Principle \(d\): Accuracy | ICO](#) (Accessed: 11 September 2025).
- ICO (2025a) *Purpose Limitation* Available at: [Purpose limitation | ICO](#) (Accessed: 11 September 2025).
- ICO (2025b) *Principle (a): Lawfulness, fairness and transparency* Available at: [Principle \(a\): Lawfulness, fairness and transparency | ICO](#) (Accessed: 11 September 2025).
- ICO (2023) *Guide to the UK General Data Protection Regulation (UK GDPR)*. Available at: [Information Commissioner's Office](#) (Accessed: 10 September 2025).
- ICO (no datea) *Getting started with data protection a step-by-step guide* Available at: [Getting started with data protection a step-by-step guide | ICO](#) (Accessed: 10 September 2025).
- ICO (no dateb) *Purpose limitation, data minimisation and storage limitation* Available at: [Purpose limitation, data minimisation and storage limitation | ICO](#) (Accessed: 11 September 2025).
- NHS Digital (2024) *Primary Care Dementia Data, August 2024* Available at: [Primary Care Dementia Data, August 2024 - NHS England Digital](#) (Accessed: 11 September 2025).
- NHS Digital (no datea) *About Us*. Available at: [About NHS Digital](#) (Accessed: 11 September 2025).
- NHS Digital (no dateb) *How we use your data*. Available at: [Your data](#) (Accessed: 11 September 2025).
- NHS England (2022) *Data Security and Protection Toolkit*. Available at: [Data Security and Protection Toolkit](#) (Accessed: 10 September 2025).



Remember UWTSD Resources...

UWTSD Library Support



Academic and InfoSkills

Our Skills programme is designed to create opportunities for students to develop their transferable academic and information skills, facilitating both their academic success and employability. The curriculum covers a wide range of topics – from finding library resources to fake news to managing your online presence.

Our team of Academic Liaison Librarians have developed a series of online Units that allow you to develop your skills anywhere, anytime, to suit you. Click the tiles below to get started:



The UWTSD Library team have provided additional support to help you to develop your research skills. These are available for you to work through at your own pace.



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives