GDPR: Implications for End of Life Care

15th June 2021

Barry Moult
IG Privacy Ltd

Guidance & Practicalities - Internal

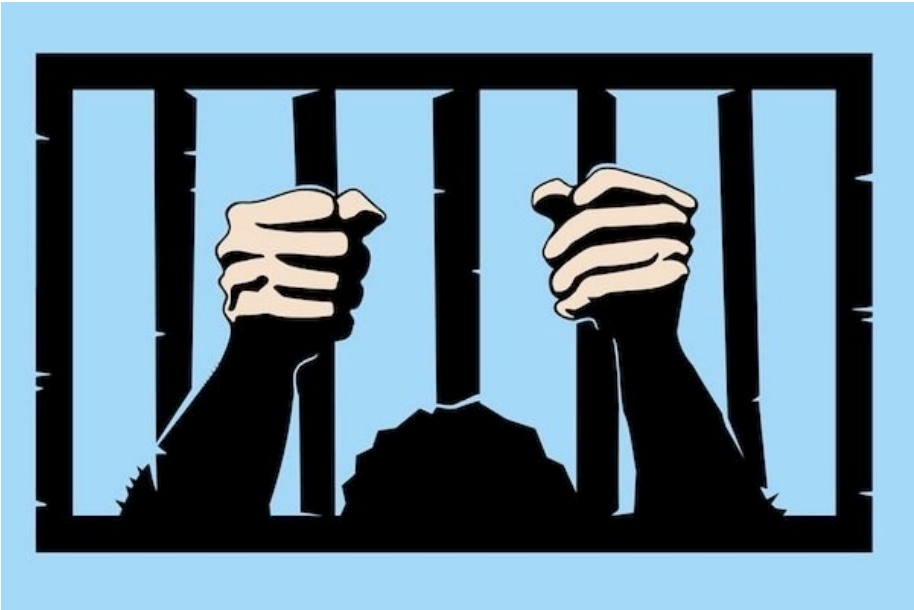
1. CEO – Accountable Officer
2. Senior Information Risk Owner
3. Caldicott Guardian
4. Data Protection Officer
5. Information Governance Team

Guidance & Practicalities - External

1. UK Caldicott Guardian Council
2. National Data Guardians Office
3. NHSX – IG Portal
4. GMC – Guidance
5. BMA – Guidance
6. Information Commissioners Office

Chief Executive Officer

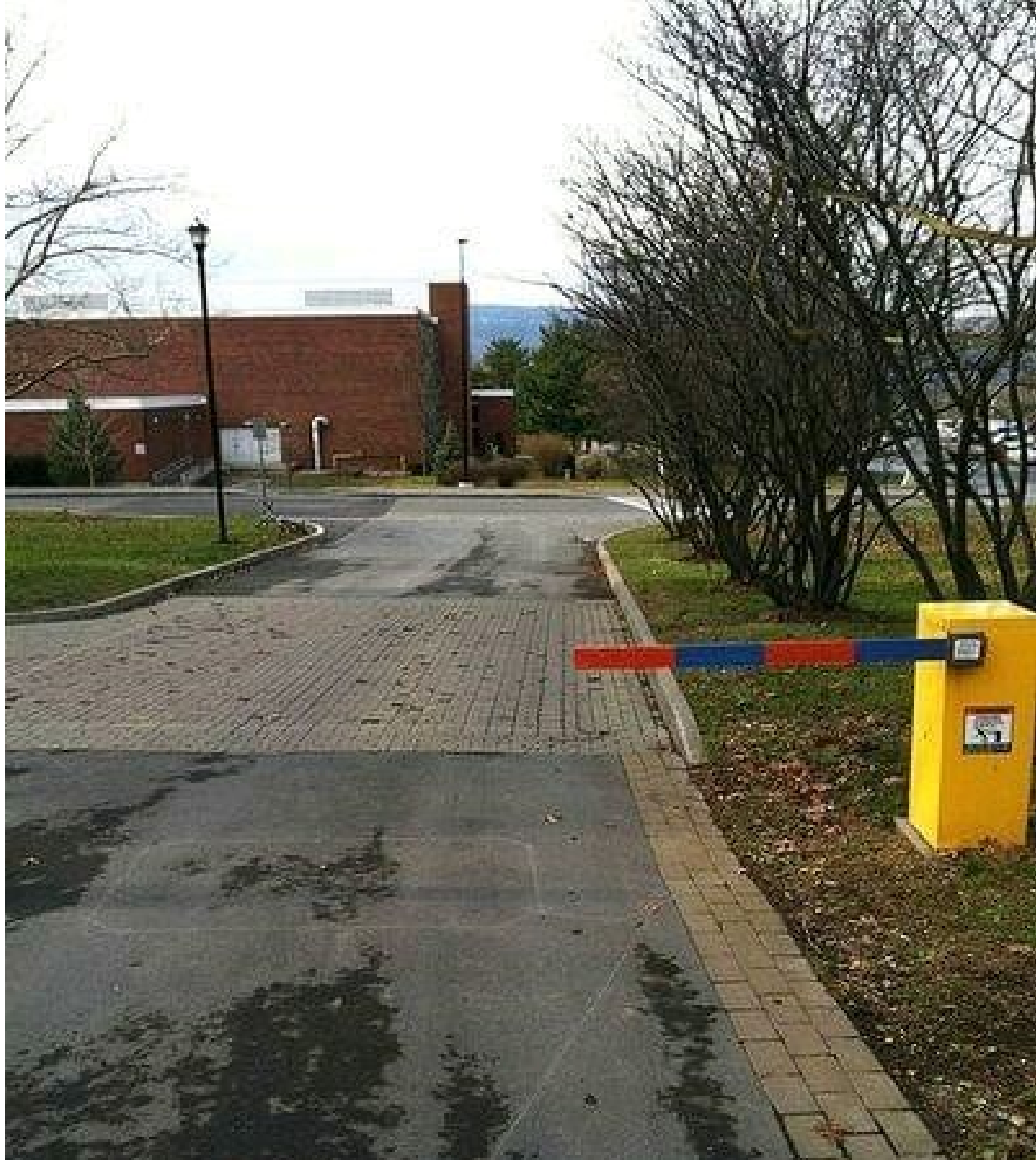
The **Chief Executive** (Accountable Officer) and **Board** have **ultimate legal accountability**



Senior Information Risk Owner

SIRO as a **board level representative** for information risk may carry *some* **liability** in the event of **breach or incident**

Responsible for compliance with the law.



Caldicott Guardian

Act as the ‘conscience’ (door keeper) for disclosure of personal and sensitive data

3 Caldicott Reports;
1997-Information Sharing.
2012-Duty to Share.
2016/17-Data Standards

Data Protection Officers

- **The DPO's minimum tasks are defined in Article 39**:
- **Inform and advise** the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

- **Monitor compliance** with the GDPR and other data protection laws.

- **Advise** on data protection impact assessments; and **conduct** internal audits.

Information Governance Team

Provide Support for the practical implementation of Data Protection and completion of the Data Security & Protection Toolkit (DSPT)

Key considerations for Information sharing in End of Life Care

Demonstrate Compliance with the Law

Relevant Legislation

- Data Protection Act 2018
- EU General Data Protection Regulation (UK GDPR) 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Environmental Information Regulations 2004
- Health & Social Care Act 2012
- Control of Patient Information Act 2002
- National Data Guardian Act 2018

Common Law duty of confidentiality

Caldicott Principles

- **Justify the purpose** for using confidential information.
- Don’t use personal confidential data unless **absolutely necessary.**
- **Use the minimum** necessary personal confidential data.
- **Access** to personal confidential data should be on a strictly need-to-know basis.
- Everyone with access to personal confidential data should be **aware of their responsibilities**.
- **Understand and comply with the law.**
- **The duty to share** information can be as important as the duty to protect patient confidentiality.
- **inform patients and service users** about how their confidential information is used

Principles of the GDPR

- **Lawfulness, fairness and transparency**
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- **Integrity and confidentiality**
- **Accountability**

Rights of Individuals

There are 8 rights of an individual. These are:

- **The right to be informed.**
- **The right of access.**
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Raising awareness in your organization

Empower staff to share and have confidence they are doing the right thing.

What will help you to do your job more effectively?

Who needs the awareness.

You?

Colleagues?

Others?

What information do you require?

Who do you require it from?

What are the hurdles?

The 6 Lawful Bases (Article 6)

1. **Consent** – individuals have given consent for their data to be processed for specific purposes.

2. **Contract** – it is necessary to process an individuals personal data to fulfill a contract you have with them.

3. **Legal obligation** – it is necessary to process personal data to be compliant with the law.

4. **Vital interests – it is necessary to process personal data to protect an individual's life.**

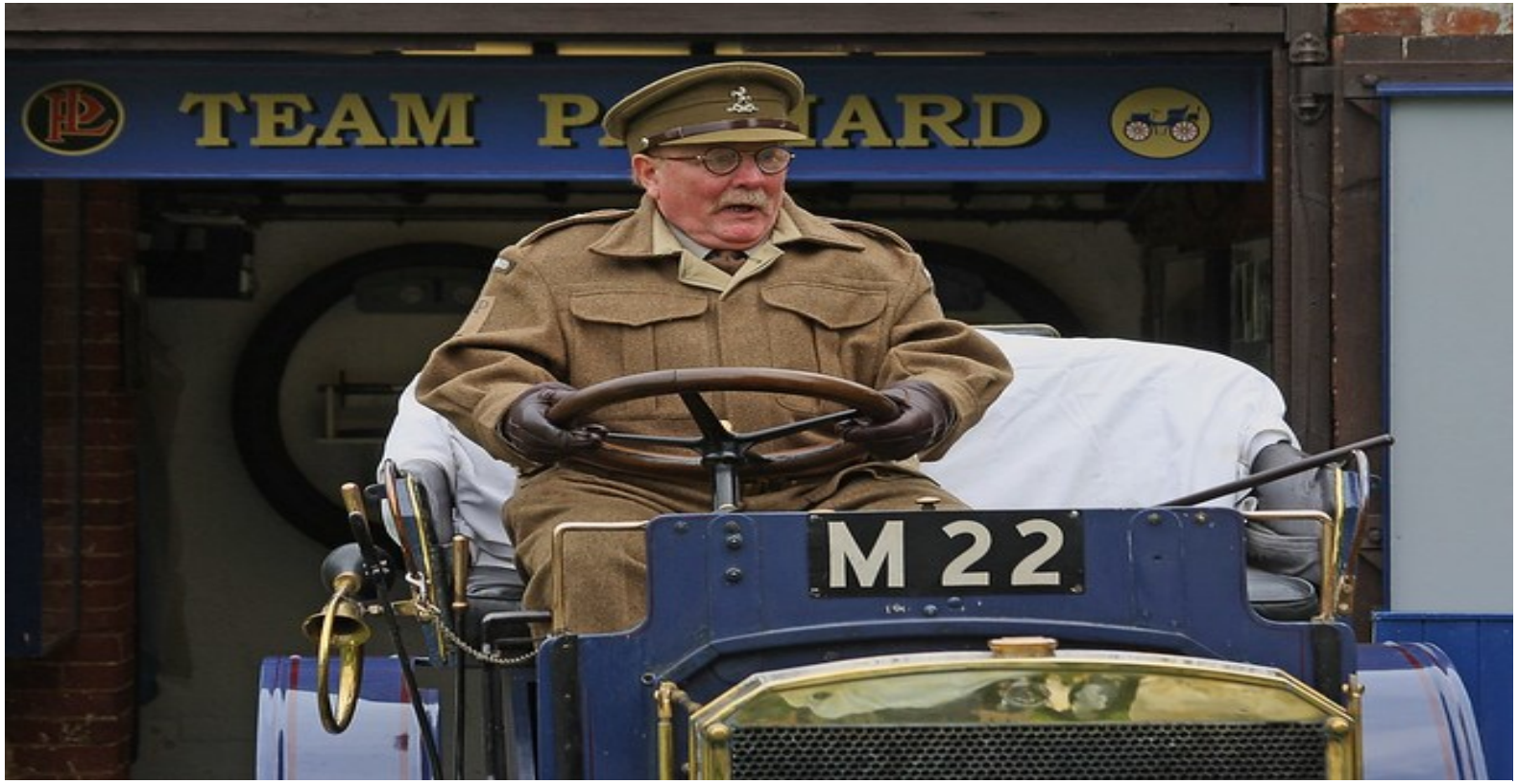
5. **Public task – it is necessary to process personal data for tasks in the public interest (this is usually government use).**

6. **Legitimate interest** – it is necessary to process personal data for your legitimate interests. You must ensure that these interests don't outweigh the rights of the individual. (assessment)

Personal data - Number 5 and 6 and

Medical Data - Exemption Article 9(2)(h)

Data Rreach Management (Reporting)



Don’t panic Mr Mannering

Personal Data Breaches

What you do about a personal data breach will depend on how great a risk that breach will be to people.

- If there is a likely risk to rights of individuals, you must report the breach to the ICO within 72 hours of the breach (72 hours from when you realise the breach has taken place).

- If there is high risk to individuals that the data is about, you must carry out duty of candour

- **When is it NOT reportable to the ICO?**

1. Contained,

2. Trusted Partner

3. Not likely to cause significant harm)

4. Encrypted devices

Privacy Notice

A Privacy Notice must include:

- Legal basis for processing
- What the data is used for
- Where data is collected from
- Where the data is stored
- Who has access to it
- Who it is shared with
- How long it is kept for
- Individual rights
- Contact details of the DPO
- Right to complain to the ICO

The Role of the Regulator - ICO

- The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals
- Issue of actions and fines following a breach of personal data
- Holds records of all Data Controllers
- Operates a helpline (chat function)
- Provides guidance pages, free leaflets.
- Issues newsletters and articles of interest

Any Questions