Ensuring Good Practice & Compliance in Health & Social Care

An Introduction

Christopher Fincken

Member UK Caldicott Guardian Council (Chair 2012-2017)
Member Inter-Collegiate & Agency National Domestic Violence & Abuse (INCADVA) Forum
Collaborative Working with the Home Office & Centre of Excellence for Information Sharing
Former Member National Information Governance Committee (CQC)
Former Participant Mental Health Crisis Review
Author of “Striking the Balance” and “Horns of a Dilemma”

Email: caldicottguardian@hotmail.co.uk Mobile 07891 641090

©C. Fincken 2018
“If you can't explain it simply, you don't understand it well enough.”

Albert Einstein
The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation – GDPR.
Evolution not Revolution
The most significant addition is the accountability principle. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity.

- [https://ico.org.uk](https://ico.org.uk)
The Sky didn’t fall in on May 25th!

Recital 4
EU GDPR
(4) The processing of personal data should be designed to serve mankind.
GDPR - Key Principles
Personal Data Shall be:

**Principle 1**
Processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);
What does Lawful Mean?

Why Isn’t confidentiality still absolute?

Information Governance (IG)
Data Protection/GDPR
Common Law of Confidence

Duty of Care
Health-Article 9 conditions

• processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

• processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

• processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
• What does Fair Mean?

FAIR PROCESSING/ PRIVACY NOTICES


NO SUPRISES!
What does Transparent Mean?

DEMONSTRATING HOW DECISIONS ARE TAKEN!
A template for answering queries

For every Caldicott Query:

• What pieces of Law have been considered? (DP, Common Law, etc.)
• What professional Guidance has been Considered? (e.g. GMC etc.)
• How have the Caldicott Principles been considered and satisfied?
• Who have I talked to?
• Is the information presented complete or inadequate?
• What is the rationale for the decision?

• What is the decision?

Write It down!
GDPR - Key Principles
Personal Data Shall be:

*Principle 2*

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);
Principle 3

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
Principle 4

Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
Principle 5

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);
GDPR - Key Principles
Personal Data Shall be:

Principle 6

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
Data Protection Officer
• All public sector organisations must have one (covered by FOI)
• Can appoint 1 DPO to multiple organisations
• Role can be part of another job – but no conflict of interest
(Cannot be CEO, SIRO, Caldicott, Head of IT etc.)

Difficult for small organisations
• Expert knowledge in Data Protection law and practice
• Can be outsourced.
• Training Responsibility of the Data Protection Officer
Demonstrating compliance

PRIVACY IMPACT ASSESSMENTS (PIA’s under DPA)

Data Protection Impact Assessments (GDPR)

• The Role of the Caldicott Guardian – Oversight?

REMEMBER ALSO TO COMPLY WITH COMMON LAW OF CONFIDENCE

©C. Fincken 2018
Demonstrating compliance

SUBJECT ACCESS REQUESTS (SARs) – No Charge

Redactions
3RD Party data
Risk of Harm
CRADLE TO GRAVE DATA PROFILE – What Data?

Some data provided by Patient’s “History”
Some Data “created” by The service (e.g. Test results)

HOW MUCH DOES THE PATIENT KNOW/THINK IS IN THEIR RECORD?
Demonstrating compliance

WHO “OWNS” THE DATA? - WHO CONTROLS THE DATA?
DECEASED RECORDS
ASSET REGISTERS
Records of Processing
Security Arrangements
Breaches
HR?

©C. Fincken 2018
Challenges

Is Cyber Security "IG" not Caldicott?

Should we record unsubstantiated "intelligence" from 3rd Parties?

To get the best from Artificial Intelligence large Data sets are needed.

Not Just IG! Caldicott Guardians need to be involved. When are patients to be told about breaches?
Where to next?

Christopher Fincken
caldicottguardian@hotmail.co.uk
07891 641090