Data Protection for small healthcare organisations

Robert Parker
Corporate Affairs

Lauren Earith
Team Manager

Liz McKay
Lead Auditor

ico.
Information Commissioner's Office

Objectives

- Help you understand the work done at the ICO
- Give you a basic understanding of the principles of data protection
- Give you an basic introduction to the General Data Protection Regulations (GDPR)
- Highlight some of the key risks to privacy compliance for health sector organisations

Introduction to the ICO

Enforcement

Issue a Civil Monetary Penalty notice

Leading to a fine ranging up to £500,000

Issue an Enforcement Notice

A formal notice requiring an organisation or individual to take the action specified in the notice in order to bring about compliance with the Act and related laws. Failure to comply with a notice is a criminal offence.

Request and agree an Undertaking with the organisation

A formal undertaking can be given by an organisation to the ICO, committing the organisation to a particular course of action or otherwise achieving compliance.

Case work and Helpline

Lincolnshire Echo

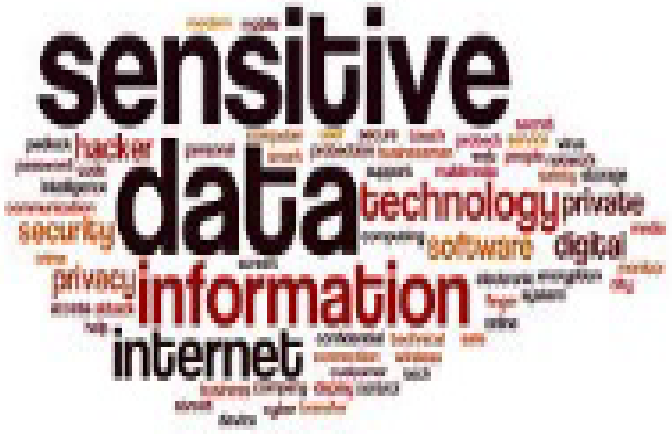
GP practice in County Armagh warned after patients' details compromised following email attack

Personal & Sensitive Personal Data

What is personal data?

So, what is sensitive personal data?

Sensitive or Special Categories of Personal Data



Defined in the DPA as data relating to:

(a) **racial or ethnic** origin
(b) **political** opinions,
(c) **religious beliefs** or other beliefs of a similar nature,
(d) membership of a **trade union**
(e) **physical or mental health** or condition,
(f) **sexual** life,
(g) the commission, or alleged commission, of **any offence**, or
(h) any **court proceedings** or sentence relating to any offence committed or alleged to have been committed.

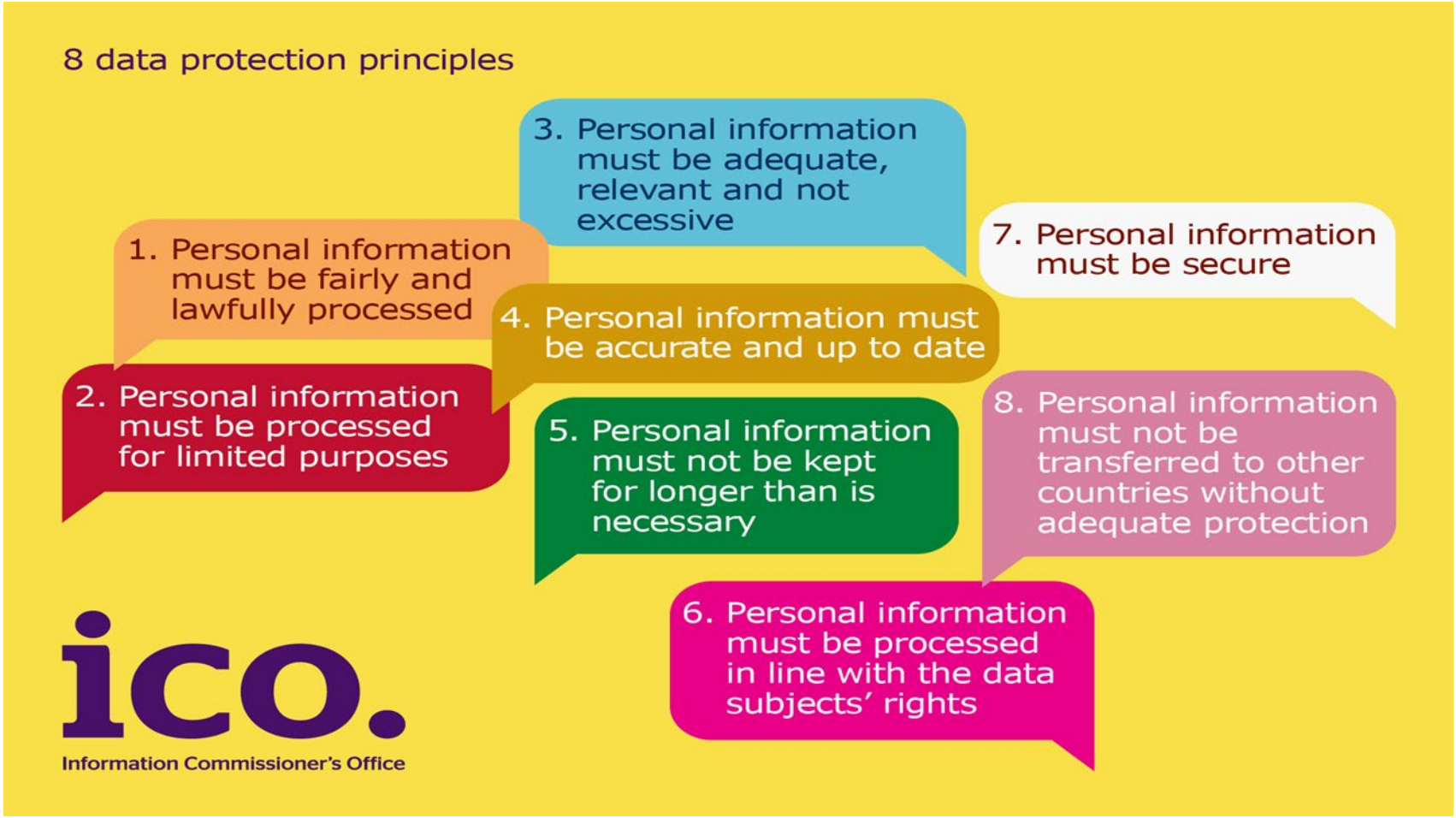
Data protection and you

• Protecting people's information rights and personal data is a front line service

• Individuals have important rights, including the right to find out what personal information is held about them

• Anyone who processes personal information must comply with the data protection principles

Data Protection Act 1998
The eight principles



GDPR Principles

Personal data should be:

(a) processed lawfully, fairly and in a transparent manner,

(b) collected for specified, explicit and legitimate purposes,

(c) adequate, relevant and limited to what is necessary,

(d) accurate and where necessary kept up to date,

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and

(f) processed in a manner that ensures appropriate security of the personal data.

Accountability is central to GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

The 1st Principle

Personal information must be

fairly and lawfully processed

Personal data should be processed lawfully, fairly and in a transparent manner

The (often neglected) 2nd principle

Personal information must be

processed for limited purposes

Personal data should be collected

for specified, explicit and

legitimate purposes

The information standards or data standards principles

They seek to regulate;

- the amount of data collected about a person by an organisation;
- the quality of that data; and
- how long it is kept for.

The “Goldilocks” principle

Personal information must be adequate, relevant and not excessive

Personal data should be adequate, relevant and limited to what is necessary

“The three bears…”

Adequate

Relevant

Not excessive

The 4th principle

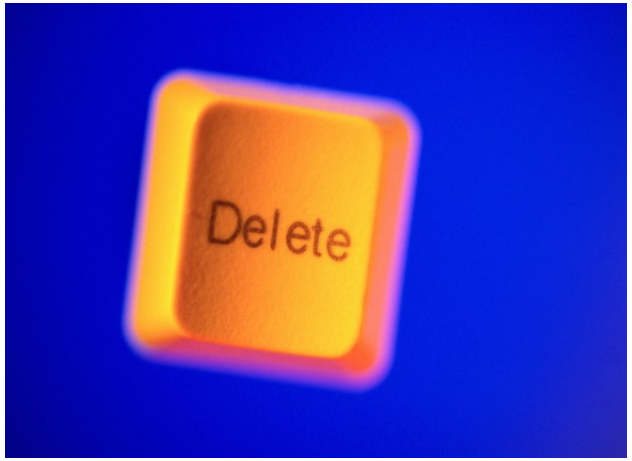
• Data will be inaccurate if it is incorrect or misleading as to any ‘matter of fact’

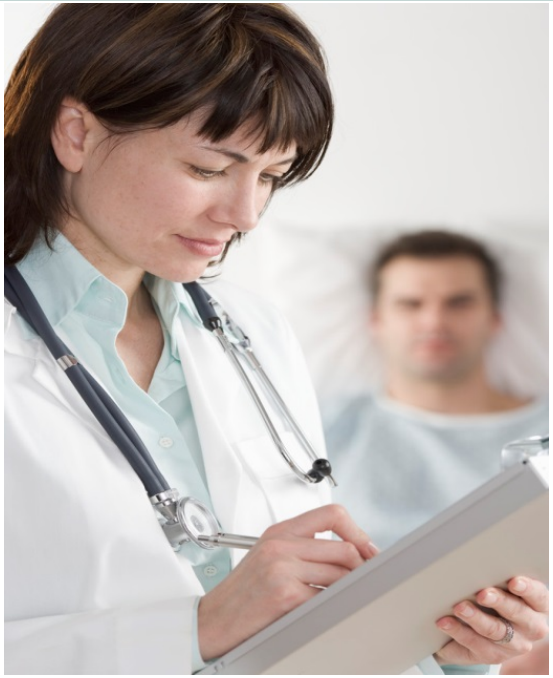
• Data must be kept up to date - where necessary

However;

• Records may contain information that is no longer ‘correct’

without breaching the fourth principle.





The 4th principle and opinions

- Opinions about individuals are personal data however generally opinions cannot be challenged under the fourth principle

- Opinions should be recorded as such and put in context where appropriate (author, date ,etc.)

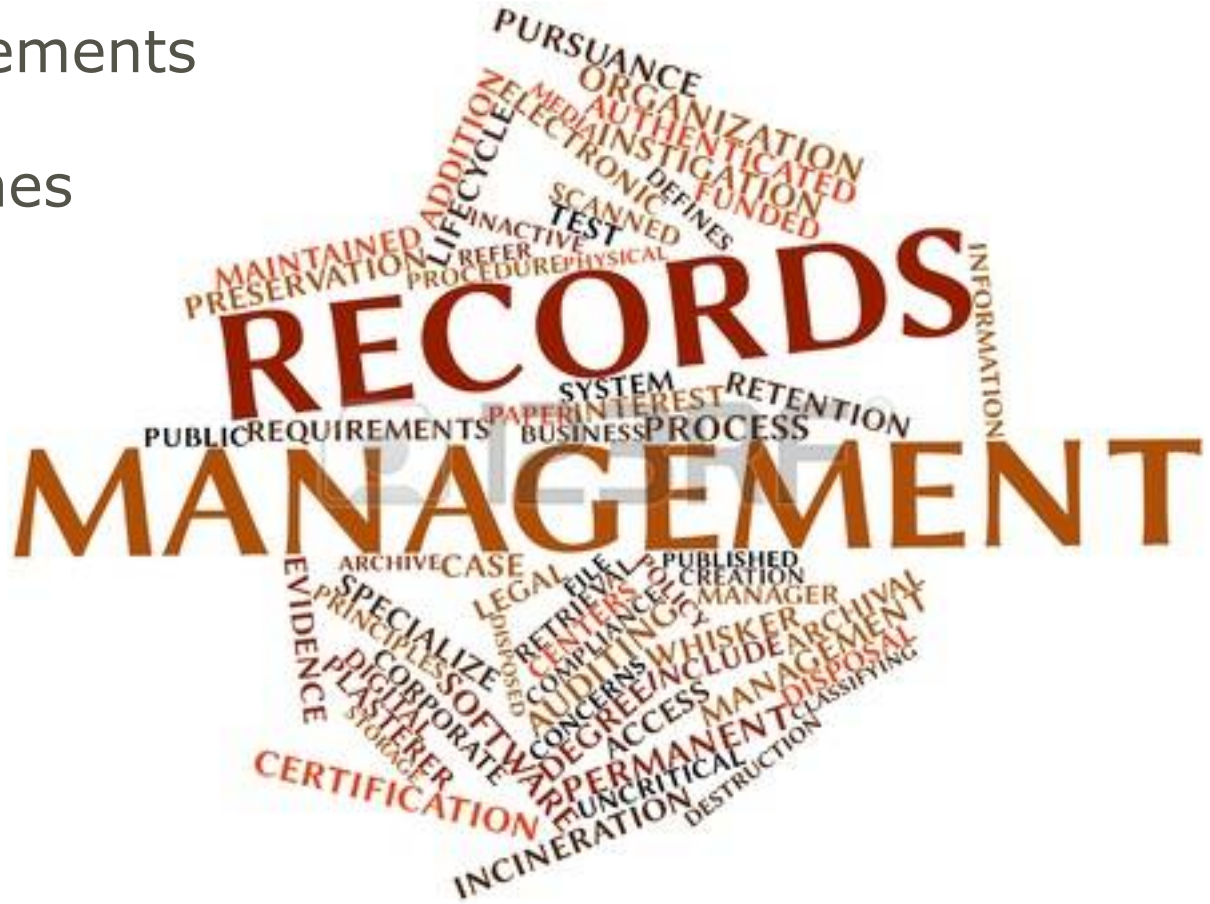
The 5th principle

Personal information must not be kept for longer than is necessary

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed

Retention

- Statutory requirements
- Industry guidelines
- Value
- Risks
- Accuracy



Other retention considerations

- Inaccuracy over time
- Weeding / deletion of information
- Statistical, research or historical information

The 6th principle

Personal data must be processed in line with the data subjects rights

- The right to know who will see and use their personal data
- The right to know why their data is being collected and what it will be used for
- The right to have copies of ALL their personal data that is being processed or held; and
- The right to have any codes or jargon within provided copies of their personal data explained to them

Rights for individuals under the GDPR

The main rights for individuals under the GDPR will be:

- subject access;
- to have inaccuracies corrected;
- to have information erased;
- to prevent direct marketing;
- to prevent automated decision-making and profiling; and
- data portability.

Subject Access Requests

The requirements for data controllers:

- Statutory timescales
- Documented procedures
- Accountability
- Disclosure file content

Subject Access Requests

The requirements for requestors:

- Requests in writing
- Proof of identity
- Administration fee
- Clarification of request

The 7th principle

Personal information must be secure

Personal data should be processed in a manner that ensures appropriate security of the personal data

Why does information security matter?

Examples of the harm caused by the loss or abuse of personal data include:

- Lost or misfiled patient test results where follow up medication had been prescribed but was never delivered (presenting a threat to life / wellbeing);
- Patient Records relating to sensitive issue being disclosed, with possibly serious implications;
- Lack of availability of vital patient data in an emergency situation.

British Pregnancy Advice Service

Date: 7 March 2014

British Pregnancy Advice Service fined £200,000. Hacker threatened to publish thousands of names of people who sought advice on abortion, pregnancy and contraception.

Abortion provider BPAS fined £200,000 for data breach

Links between the principles

Compliance with these principles is closely linked. If you breach one principle it is likely you will also have problems complying with the others.

These principles set standards for the ‘quality’ of personal data

To comply with these principles you need to take steps to ensure the accuracy of data that you hold and regularly review your records

General Data Protection Regulation

It is not back to the starting line….

Key risks for you as SMEs in the health sector

ico.
Information Commissioner's Office

Information security risks

- Systems accesses (new starters and leavers) not reviewed or adjusted as required

- No clear desk policies in operation or work place security checks completed

- Security encryption not in place or out of date for all equipment including removable media

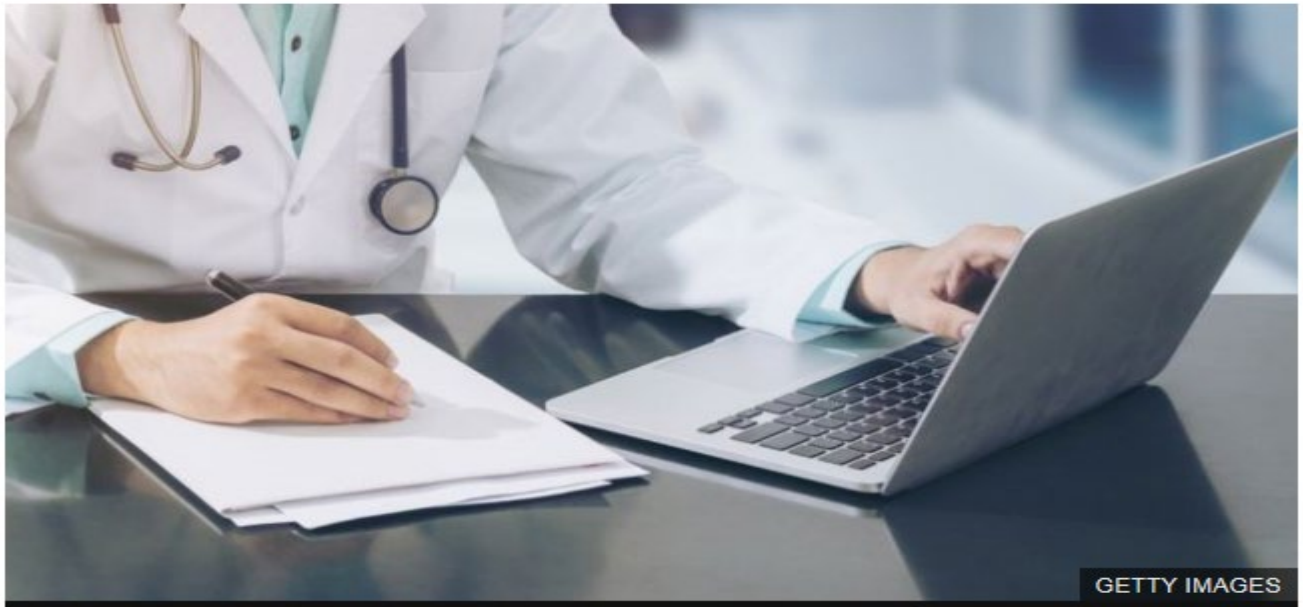
- No Physical security protocols / systems / entry controls in place

- No Password security procedures in place

- Lack of effective security incident monitoring or reporting

Bupa data breach affects 500,000 insurance customers

13 July 2017 | Technology



No medical data was made vulnerable in the breach, Bupa said

A Bupa employee inappropriately copied and removed information relating to 547,000 international health insurance plan customers, the company has said.

Manual records risks

- Logging, tracking and movement of manual records
- Secure storage areas for live and archived records
- Maintaining the data quality of records
- Lack of staff training in records management

Subject access risks

Staff not fully aware of what a Subject Access Request (SARs) is and how to deal with one

SAR redactions and exemptions not logged or reported.

SAR response dates not met

Want to know some practical ways to avoid the key risks?

Attend our workshop near you!!!

Get in touch

Chat with our advice services team via our

- **Live chat** at ico.org.uk; or
- Call our **helpline** on 0303 123 1113.

Keep in touch

Subscribe to our monthly e-newsletter at www.ico.org.uk

Follow us on:

@iconews

/iconews