National Care Association

GDPR

Lynne Omar

Senior Consultant

Newcastle

14th June 2018

What is GDPR?

GDPR refers to The General Data Protection Regulation.

GDPR will come into effect on the 25th of May 2018 and will replace the Data Protection Act 1998. It will regulate how organisations process personal data

Does GDPR apply to care homes?

Yes. It applies to all companies processing personal data where the data subject resides within the European Union, except when processing takes place for law enforcement purposes.

Cura Systems

What is personal data?

Personal data is defined as information which relates to a living individual who can be identified from that information or from that information and other information which is in the possession of, or likely to come into the possession of the individual or company viewing the information.

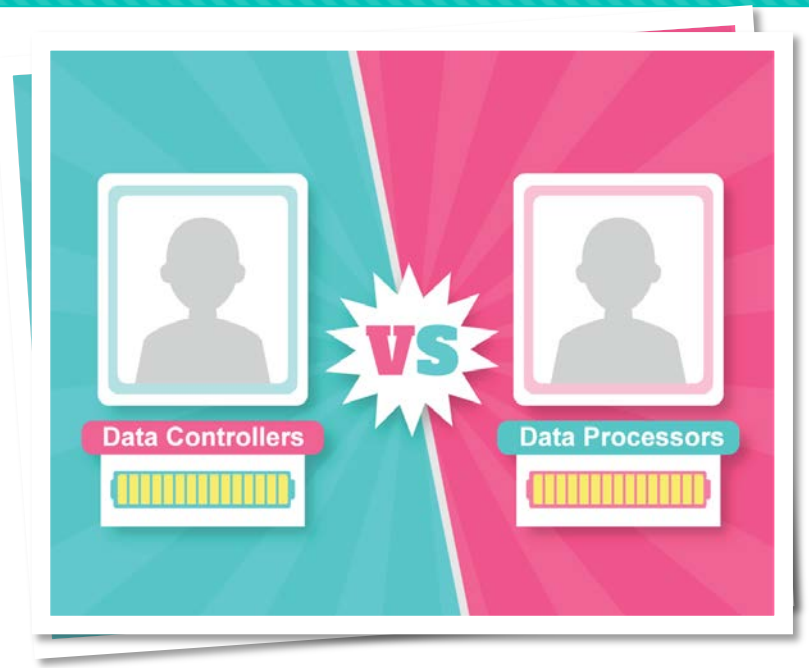
Some examples of personal data items which, either on their own or in combination, can identify an individual include:

Information can be about staff, residents, residents' family members, visitors or other companies' contact details where they relate to an individual rather than being generic.

- Name (Middle initial increases the risk of identification. Includes signatures in some instances)
- Address
- Date of Birth
- Other dates (i.e. death, diagnosis)
- Occupation
- Gender
- National Insurance number
- Hospital or NHS number (NHS number vs DOB)
- Email address (Includes work in some instances)

Data Controllers vs Data Processors

- A data controller determines the purpose, conditions and means of the processing of personal data.
- A data processor simply processes personal data on behalf of the data controller.
- Article 26 of GDPR comments that; "*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers*".



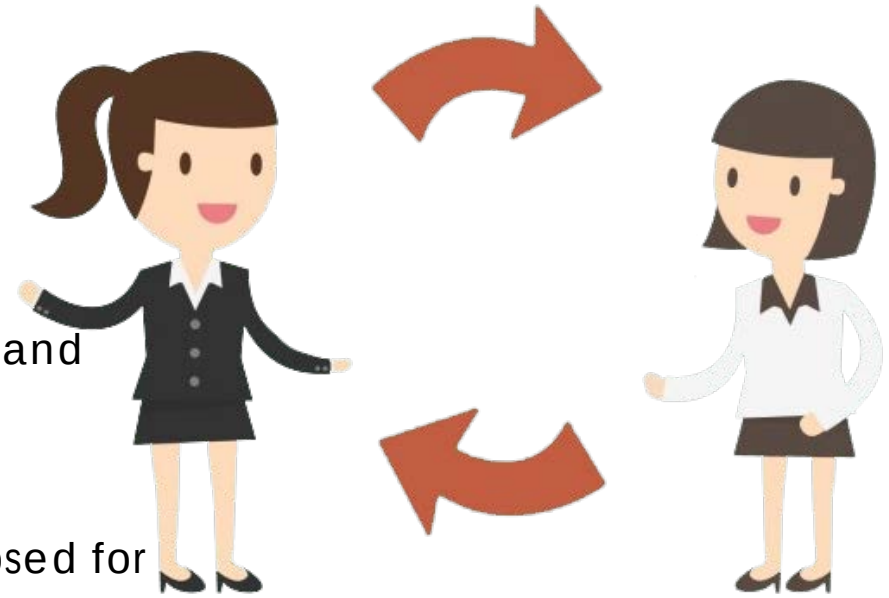
Lynne.Omar@Cura.Systems

Cura Systems

What are the main differences between GDPR and the Data Protection Act 1998?”

GDPR;

- Broadens the definition of personal data
- Provides updated principles
- Increases the responsibilities of data controllers and data processors
- Enhances the rights of data subjects
- Enables greater monetary penalties to be imposed for failure to comply



Lynne.Omar@Cura.Systems

Cura Systems

Will care homes still need to register with the ICO?

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights

When the new data protection legislation comes into effect next year there will no longer be a requirement to notify the ICO in the same way.

However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

The size of the data protection fee will still be based on the organisation's size and turnover and will also take into account the amount of personal data it is processing.

The new model will go live on 1 April 2018.

Lynne.Omar@Cura.Systems

Cura Systems

Appointment of a Data Protection Officer

Do all care homes need to appoint a Data Protection Officer (DPO)?

Article 37(1) of GDPR states that organisations need to appoint a DPO if "*the core activities of the controller or the processor consist of processing on a large scale of special categories of data [...] [or]data relating to criminal convictions and offences*".

Earlier drafts of the GDPR limited this requirement to companies with more than 250 employees. However, the final version has no size restriction, meaning it can apply to small businesses too if they process large amounts of special categories of data or on data relating to criminal convictions.

Lynne.Omar@Cura.Systems

Cura Systems

Appointment of a Data Protection Officer

If you appoint a DPO, you are required to notify the ICO of the appointed DPO's contact details

Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

If you do not appoint a DPO, your processors may still need to.

Lynne.Omar@Cura.Systems

Cura Systems

Lawful processing; Due diligence

Article 28 of GDPR places an obligation on a data controller to only use data processors that are able to demonstrate compliance with GDPR.

Therefore, data controllers should carry out due diligence on any processors it uses to ensure that they are also GDPR compliant. Due diligence can include;

- Requesting copies of the company's data protection policies and privacy notices.
- Asking for a description of the company's IT Business Continuity Plan.
- Asking for a description of the company's data protection audit processes concerning physical and technical security.
- Asking for a description of the company's subject access request processes.
- Asking for a description of the company's breach reporting processes.
- Ensuring that staff know what a personal data breach is and are adequately trained on data protection matters
- Confirmation of the ability to rectify or erasure data in accordance with GDPR

Lynne.Omar@Cura.Systems

Cura Systems

What are the GDPR Principles and how can my care home comply with each one?

Cura Systems

What are the principles within GDPR?

Data Protection Act Principles

Personal data shall be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Relevant and sufficient for the purpose
- Accurate and kept up-to-date
- Kept for as long as necessary and no longer
- Processed in line with the individual's rights
- Kept secure
- Only transferred with other countries with adequate protection (EEA)

GDPR Principles

Personal data shall be:

- Processed fairly, lawfully, and in a transparent manner
- Collected for specified, limited purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up-to-date
- Kept in a form which permits identification for as long as necessary and no longer
- Processed in a manner that ensures appropriate security

Examples of explicit consent from Information Governance Alliance (IGA)

Form of consent	Unambiguous?	Explicit?
At an event sign-in, participants are informed that the organisers would like to use their registration details for specified types of profiling and are asked (verbally) whether they consent to such processing	Yes, consent may be given verbally. However, the organisers may wish to consider how the consent can be documented with greater certainty, particularly in light of the GDPR's accountability requirements	
Employees are informed that photographs will be being taken in a section of the building during a particular time and that such photos will be included on the company's intranet. Employees, having been so informed, decide to go to the area in which photographs are being taken	Yes, consent may be inferred from employees' actions in going to the areas of the building in which photographs are being taken during the relevant times	No, whilst consent may be inferred from the employees' actions, it cannot be said to be explicit
A social media website requires users to provide certain personal data in order to participate on the site. The site contains a notice, accessible in the privacy section, indicating that, by using the site, users are consenting to their data being processed by third parties to deliver them marketing information	No, the GDPR is clear that inactivity cannot constitute consent. This is consistent with the "no doubt" analysis: ongoing use of the site may indicate consent to the processing, but may also mean users have not read the notice. As there is doubt as to users' intentions, ongoing use of the site cannot constitute unambiguous or explicit consent	
An online retailer offers the opportunity to opt-out of certain processing by unticking a pre-ticked box during the order process	No, as is the case under ICO guidance, the GDPR is clear that consent cannot be obtained through pre-ticked boxes	

Informed consent

Consent needs to be informed.

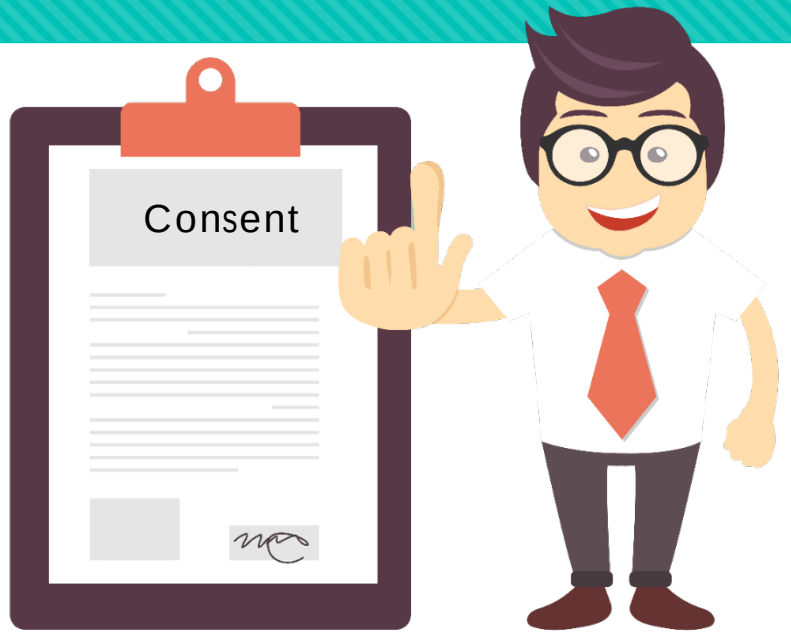
This links in to CQC and Care Inspectorate requirements. For example; the Health and Social Care Standards: My support, my life[Scotland] (June 2017) comments that service users should be able to state the below;

- Be included: "I receive the right information, at the right time and in a way that I can understand. I am supported to make informed choices, so that I can control my care and support"
- Responsive care and support: "My care and support adapts when my needs, choices and decisions change."
- Wellbeing: "I am supported to make informed choices, even if this means I might be taking personal risks."

Health and Care Professions Council's Guidance on Confidentiality (2017) comments that "*By 'informed', we mean that the service user has enough information to make a decision about whether they give their permission for their information to be shared with other people*".

Cura Systems

Documenting consent



CQC Regulation 17(2)(c) states that accurate consent records must be kept and "*include when consent changes, why the person changed consent and alternatives offered*".

This links into to accountability requirements under GDPR to evidence compliance with GDPR.

The ICO recommends that documentation should include "*who consented, when, how, and what they were told*".

The Electronic Communications Act 2000 provides legal recognition for electronic signatures and the process under which they are generated, communicated and verified.

Cura Systems

How can technology ease the path to my care home's GDPR compliance and improve customer confidence?

Lynne.Omar@Cura.Systems

Cura Systems

Other reasons to go digital

Weren't we safer with paper?

Paper is;

- Not secure
- Can lead to data breaches
- Costly to track who has copies
- Time to find what you are looking for
- Ineffective
- Multiple copies can be dangerous
- Cumbersome archives
- Easily lost

Lynne.Omar@Cura.Systems

Cura Systems

CQC and technology

Technology provides care homes with greater **transparency, visibility & control.**

Within their published documented *Safe Data, Safe Care*, CQC comment using technology "is solving many data security issues". Moreover, CQC have updated their key lines of enquiry for adult social care services in November 2017 to consider technology.

Lines of enquiry;

- **Effective: E1.3** – How is technology and equipment used to enhance the delivery of effective care and support, and to promote people's independence?
- **Responsive: R1.6** – How is technology used to support people to receive timely care and support? Is the technology (including telephone systems, call systems and online/digital services) easy to use?
- **Well-led: W4.6** – Are information technology systems used effectively to monitor and improve the quality of care?

Lynne.Omar@Cura.Systems

Cura Systems

CQC and technology

Scoring and ratings;

- E1: Are people's needs and choices assessed and care, treatment and support delivered in line with current legislation, standards and evidence-based guidance to achieve effective outcomes?
  - The outstanding score includes "*technologies are used to support the delivery of high quality care and support*".
- E6: How are people's individual needs met by the adaptation, design and decoration of premises?
  - The good score includes "*The service uses technology and equipment to meet people's care and support needs and to support their independence".*
- C2: How does the service support people to express their views and be actively involved in making decisions about their care, treatment and support as far as possible? –
  - The outstanding score includes "*Staff use a variety of tools to communicate with people according to their needs, which may include using new technologies. Staff find innovative and creative ways to communicate with each person using the service*".
- R1: How do people receive personalised care that is responsive to their needs?
  - The outstanding score includes "The service has an innovative approach to using technology."
  - The good score includes "Technology used in providing the service is easy to use and accessible to the people and staff who use it. It promotes timely and responseve care and support".

http://www.cqc.org.uk/sites/default/files/20171020-adult-social-care-kloes-prompts-and-chaacteristics-showing-changes-final.pdf

Lynne.Omar@Cura.Systems

Cura Systems

Technology and GDPR

- Information tends to be clearer to read and understand, which supports correct treatment and data accuracy (right of **access** in clear language and principle 4 of **accuracy**).
- It is easier to keep information up-to-date as it is all in one place and you can link records (Principle 4 of **up-to-date** data).
- It is easier to document evidence, such as audit trails and documented consent (**accountability**).
- It is easier to comply with SARs within timeframe as information (right of **access**).
- It is easier to share data (right of data **portability** and **access**).
- You can impose retention alerts and mandatory fields (Principle 5 of **retention** and Principle 3 of **adequate** and **necessary**)
- It is easier to keep data secure (Principle **6**);
  - Authorised access (which is easier to control and can be more granular) for confidentiality and integrity concerns (support compliance with Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 of authorised access)
  - Ensures data is available when needed (supports compliance with Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 9 of data availability to staff when needed)
  - Data is backed-up (which supports business continuity as well as prevents care homes from being victims to ransomware attacks).

Lynne.Omar@Cura.Systems

Cura Systems

Things to look for from a technology provider

The Company

GDPR compliance (refer to due diligence) and fast support services

The Product

- Access controls (to ensure confidentiality and integrity of data)
- Audit capabilities (logins, amendments to resident and staff data, document downloads)
- Ability to quickly access erase and rectify data (in line with individuals' rights)
- Ability to document consent when consent is relied upon (including audio consent)

Lynne.Omar@Cura.Systems

Cura Systems

What are the consequence for care homes for failure to comply and how should care homes identify, manage and report breaches of GDPR?

Lynne.Omar@Cura.Systems

Cura Systems

Lynne.Omar@Cura.Systems

Cura Systems

Email breach examples

The situation - Mr. Foster has recently been diagnosed with depression and has joined a support group to help him through his care. The organisation emails information to support group members each month. Recently, they have started to receive emails and phone calls from individuals who are upset about the disclosure of their names and email addresses to more than 500 people.

The organisation's reaction - The organisation undertakes an investigation and finds that a new member of staff had sent out the email. They had mistakenly put the list of all the support group members' email addresses in the 'CC' field – rather than the 'BCC' field – of all the individual emails.

Consequences - Everyone who received the email could identify who was a member of the depression support group. The investigation also finds that all existing staff members involved in sending out emails knew what to do, but had not supervised the new member of staff.

Phone breach example

The situation - Joe, a practice manager, receives a call from a local hospital requesting information about Mrs Smith, one of the practice patients. He knows she has been referred to that hospital for cancer investigation so he gives the information to the caller.

The result - The next morning, Mrs Smith phones the practice and tells Joe that her brother-in-law has information about her health that he can only have obtained from the practice. At that point, Joe realises he had no proof that the previous day's call was from the local hospital.

Lynne.Omar@Cura.Systems

Cura Systems

What best practices can my care home staff follow to reduce the risk of a breach occurring?

Lynne.Omar@Cura.Systems

Cura Systems

Staff Awareness

Staff awareness is a key element in reducing the risk of a data breach occurring.

Should a breach take place, one of the first things the ICO will ask is whether staff undergo regular data protection training. Good data protection training can mitigate an enforcement action and could put responsibility onto the individual member of staff in certain circumstances.

You should consider appropriate training levels for different staff and ensure compliance with training is effectively monitored and documented.

Lynne.Omar@Cura.Systems

Cura Systems

Best Practice Examples

Passwords - Your password(s) are specific and identifiable to you. Do not shared with other people.

Some password tips:

- Ensure your passwords are 9+ characters
- Never reuse a password for different accounts. Failure to do this means that, should your password become compromised, all your accounts are put at risk rather than just one.
- Place symbols in the middle of words (Exa#mple) rather than after (Example#)
- Do not overcomplicate passwords as this makes them hard to remember. 4 random, non-common words (SolitairDrumstickCrescendoChaos) is more secure than commonly misconceived 'secure' passwords such as PassW3rd!.
- Consider a phrase you like, or song lyric, and use the first letters of each word rather than a dictionary word.
- Consider a code to make remembering multiple passwords easy. Such as always playing a fullstop as the 3rd character and the capitalizing the 5th.
- Avoid using information readily available or easily guessed, such as your DOB or pet's name.

Lynne.Omar@Cura.Systems

Cura Systems

Best Practice Examples

Lock your computer when you leave it unattended and be aware of the direction it is facing to prevent someone viewing the content

The Importance of locking computer screens

- Locking your computer is an easy, yet often overlooked, way to keep information safe. Though locking your computer each time you leave your work desk, even if you are just running to fill up your water bottle, may feel inconvenient, it is important to take the time to do so. When your computer is unlocked and unattended, you are leaving information open to anyone walking by (other staff and members of the public) and enabling access granted to you for the purpose of your job role to be exploited
- Due to the confidential and sensitive nature of the information we hold, if clients notice unattended computers are being left unlocked, they may start to question the credibility of our company in protecting their information.
- Furthermore, a common misconception is that locking your computer ONLY protects against internal threats. Myth busted! Not only does it protect us from internal threats, but it also helps by delaying external attacks.
- Computer security is important in all locations, both within public areas and within staff offices or homes Locking your computers protects information against unauthorised disclosure and alteration. Moreover, leaving your computer unlocked places yourself at risk of other persons sending emails in your name
- Locking your computers can prevent inconveniences. For example, when your computer is not used for a while the monitor may dim or go off to save power. However, that does not mean that the computer is off. If you don't lock your computer when not in use, yourself or a stranger may come and press a key like delete, enter or space to wake up the computer. These buttons can sometimes trigger an action such as submitting a form or executing a command. For example, when the delete key is used to wake up the computer, you may end up losing an important file or some text in a document. If you lock your computer when not using it, such instances cannot occur.

Lynne.Omar@Cura.Systems

Cura Systems

Best Practice Examples

- Ensure equipment and confidential documents are stored within a locked boot when leaving them unattended in a car. (Insurers love to say if it is visible you are 'inviting' theft in!)
- Always connect to the VPN when using confidential information and store electronic information on the secure network (Z drive) **Do not save documents to your desktop or device**! Short cuts can be used instead. This makes information less accessible in the event of lost or stolen equipment, and also ensure all information is safely backed up
- Never use a free public Wi-Fi connection on work equipment. Hackers will often create fake hotspots for the purpose of unauthorised access to confidential information.
- Limit what internet sites you are accessing on work devices to trusted sites.
- Never publish confidential information online.
  - Tip: Don't put your belongings at risk by promoting that you're on (or going to be on) holiday on Facebook until you are back. Doing so, even if you've limited your privacy settings, puts your valuables at risk of theft and will void any insurance should one occur.
- Don't disable the antivirus protection software
- Always securely dispose of confidential information (shred paper documents)
- Use discretion when talking, both face-to-face and on the telephone, and take in to consideration the environment you are in

Lynne.Omar@Cura.Systems

Cura Systems

Best Practice Examples

- Email is an unsecure means of information transfer. Therefore, no confidential or personal data should be included in a body of an email.
  - Either limit the information so it is no longer confidential or personal (identifiable) if possible, or place the information you wish to send in a Word document and encrypt that Word document before attaching it to the email.
  - If clients want to send you identifiable residential information, encourage them to also encrypt it.
- Remember, emails are retained by the company for legal retention requirements and can be released under information requests if relevant. Therefore, if you have been unprofessional about another staff member and they make a legitimate request for a copy of that email, they can request you face disciplinary action.
- Don't register your work email address with 3rd party websites for personal/private reasons (this includes online shopping or schools)
- Encrypt any equipment that contains personal or confidential information (such as USBs)
- Do not use unauthorised USB drives and avoid plugging in any non-approved devices to charge via a USB cable.

Lynne.Omar@Cura.Systems

Cura Systems

Best Practice Examples

Staff must be aware of the associated risks of receiving emails such as:

- **Phishing** - a way of attempting to acquire confidential and sensitive information such as usernames, passwords and credit card details by websites masquerading as legitimate organisations.
- **Malware/Virus** - malicious computer programs designed to gather information that leads to loss of privacy or exploitation and gain unauthorised access to computer systems.

Do not open suspect attachments or click on links from unknown senders.

- If you receive an email that is clearly not genuine, please do not open or click on links and instead right click it and mark it as Junk

Refer to further guidance within the previously covered section Security and 'suspect emails

Lynne.Omar@Cura.Systems

Cura Systems

What other vital data protection legislation should I be aware of to support my care home's GDPR compliance?

Lynne.Omar@Cura.Systems

Cura Systems

The Computer Misuse Act 1990

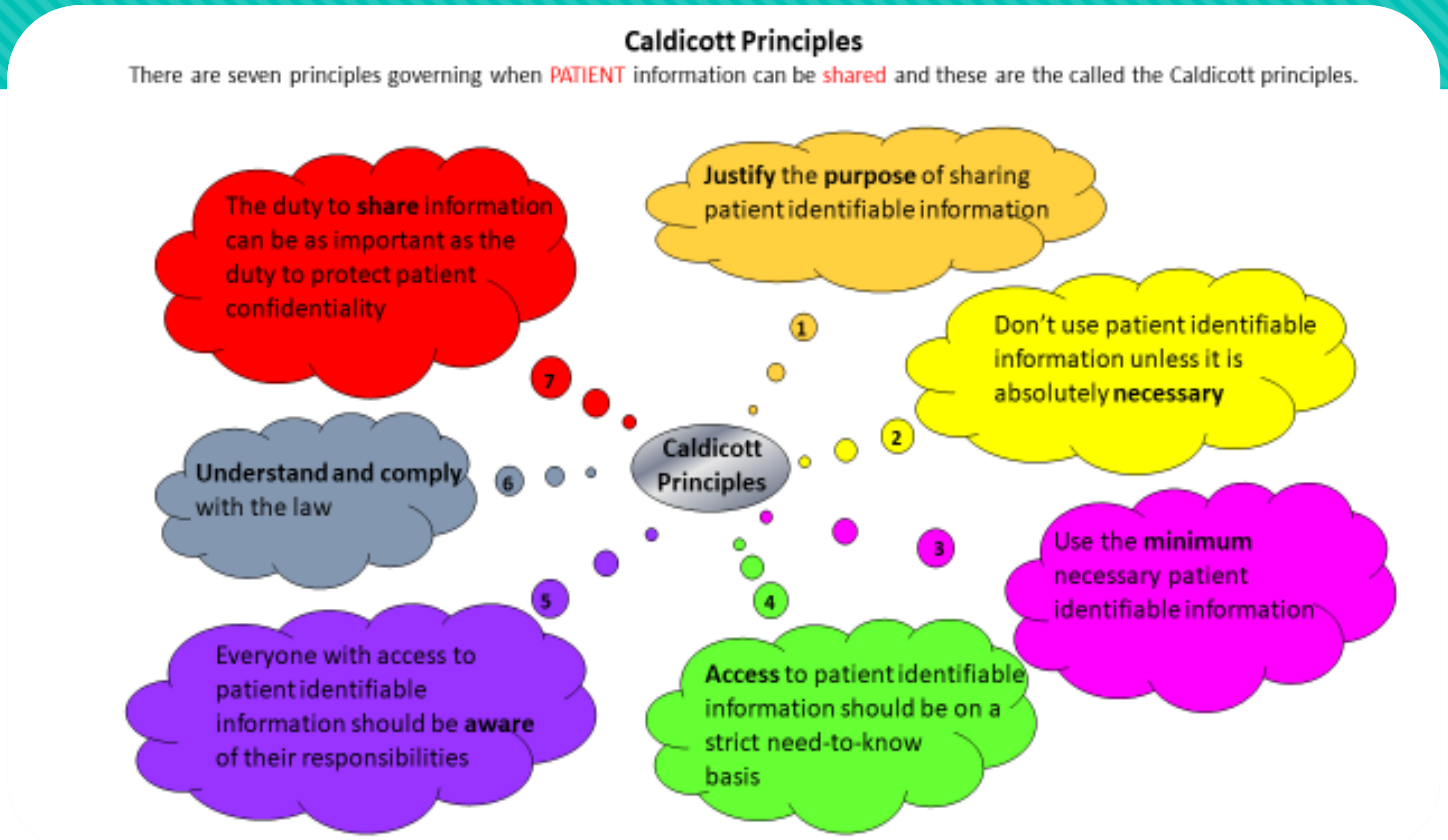
Under the Computer Misuse Act 1990, the following are offences:

- Unauthorised access to computer material (section 1);
- Unauthorised access with intent to commit or facilitate commission of further offences (section 2); and
- Unauthorised modification of computer material (section 3).
- The maximum penalty for the section 1 offence (unauthorised access to computer material) is two years' imprisonment and a fine. For a section 2 offence, the maximum penalty is 5 years' imprisonment and a fine. For a section 3 offence, the maximum penalty is 10 years' imprisonment and a fine.

Lynne.Omar@Cura.Systems

Cura Systems

Caldicott Reports 1997, 2012 and 2016



Lynne.Omar@Cura.Systems

Cura Systems

Summary and *key steps to GDPR compliance* checklist review

Lynne.Omar@Cura.Systems

Cura Systems

25 key steps to GDPR compliance checklist review

1. Identify all of your processing activates
2. Establish and document your legal basis for processing data
3. Identify;
    A. Where you are the data controller,
    B. Where you are a joint controller,
    C. Where you are a data processor, and
    D. Where you utilise a data processor
4. Confirm that any identified data processors are GDPR compliant (Due diligence)
5. Confirm that contracts are in place with all data processors and are GDPR compliant
6. Consider the need for contracts when sharing with other data controllers or whether to add liability disclaimers.
7. If not already done; consider the appointment of a Data Protection Officer
8. Check if your consent processes need updating in line with GDPR and The Bill (Age/informed/explicit/recorded)

Lynne.Omar@Cura.Systems

Cura Systems

25 key steps to GDPR compliance checklist review

9. Develop/update privacy notices (Staff/Service Users/Visitors/Website Viewers/Other companies' contacts) to be GDPR compliant
10. Ensure your direct marketing procedures are compliant with GDPR and PECR
11. Ensure adequate data quality checks are in place
12. Ensure data is kept in line with retention requirements
13. Consider the development or updating of policies
14. Review your data security measures in place and assess if there are any areas for improvement
15. Review how data is shared via email and if procedures or guidance need to be provided (such as on encryption or limiting data)
16. Classifying your data
17. Ensure staff are aware of the risk of social media

Lynne.Omar@Cura.Systems

Cura Systems

25 key steps to GDPR compliance checklist review

18. Review the risk of re-identification of pseudonymised and Anonymised data
19. Review or develop audit processes to monitor GDPR compliance
21. Ensure your subject access request process is updated in line with GDPR
22. Ensure you are able to rectify and erase data when requested and have processes in place to handle such requests (including notifying any third party recipients of the data)
23. Assess your technology systems (or the benefit of introducing one)
24. Develop and populate an Information Asset Register and Review your change management and risk assessment processes (DPIA)
25. Implement procedures to detect, report and investigate data breaches and raise awareness of these

Lynne.Omar@Cura.Systems

Cura Systems

Thank you

Cura Systems