www.personcentredsoftware.com
care@personcentredsoftware.com
01483 604108

Are you ready for GDPR?

By 25th May 2018 most organisations will have had to become compliant with the new General Data Protection Regulation (GDPR).

What has changed with GDPR?

GDPR replaces the Data Protection Act 1998 and is a piece of legislation with much more power to protect people's data and will be enforced by the UK Information Commissioners Office (ICO).

The regulation firmly puts control back in the hands of the data subjects (the people the information is about) and puts significant new corporate requirements in place to ensure that all data processors (any entity or individual that processes personal data on the controller's behalf) and data controllers can meet their data security obligations.

Evidence how compliance is achieved

Under GDPR, you have to not just be compliant but be able to evidence how compliance is achieved. To become compliant with GDPR it is necessary to have a reason for holding personal data, and that reason must be documented.

New rights and enhanced protection

GDPR has not been created to prevent sharing of data but for the enhanced protection for people's personal and sensitive data, such as the 'Right to be Forgotten'. The new accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility. The ICO lists several ways that data controllers can prove that they comply, such as carrying out data protection impact assessments (DPIAs) to evaluate why the personal data is being processed and any risks and safeguards for mitigating the risks.

Tougher penalties

The penalty for non-compliance is also more severe with potential fines of up to €10m or 2% of your organisation's turnover. Failure to report a data breach can attract fines up to €20m or 4% of turnover, impact on your reputation, and threaten the safety and wellbeing of the people you support.

www.personcentredsoftware.com
care@personcentredsoftware.com
01483 604108

Does GDPR apply to care providers?

Yes. GDPR applies to anyone that processes personally identifiable data about any individual. 'Processing data' includes storing, writing and reading information. This is the case whether they are on paper or electronic records. Care providers have sensitive data stored, updated and read in care plans, along with other personally identifiable records in medical records and personal care preferences. Care providers may hold data on prospects, clients, service users, staff or contacts.

How will GDPR affect care providers?

Care providers will have had to think carefully about how record-keeping may need to change to become compliant with GDPR. The following paper-orientated systems are difficult to maintain with GDPR as the regulation has introduced an additional layer of documentation for you to evidence how data is managed.

- **Manual filing systems** – all manual records containing personal data applying to staff or service users are included within GDPR. This means filing systems and paper care plans are affected, as are daily records and charts kept in a folder.

- **Back up to USB drive and tape** - due to the new accountability requirement, older computer systems backups and replication to USB drive or tape may not be compliant with GDPR as they contain just as much personal data and are subject to the same regulations.

- **Printing from a computer system** - printing a care plan from a computer system means there are both 'manual' and 'automated' copies and, under the new regulation, both need documentation to show how they are processed.

PERSON CENTRED SOFTWARE
MOBILE CARE MONITORING

www.personcentredsoftware.com
care@personcentredsoftware.com
01483 604108

How can care providers prepare for GPDR?

Things to do to prepare

- Document what data you are holding on whom and why
- Define your company's Privacy Policy
- Appoint a Data Protection Officer
- Define your Digital Strategy and review it regularly
- Ask questions of your software provider (or prospective partner)
    - Where is your data?
    - How is it managed?
    - How is it protected?
- Educate and train staff on data protection and handling
    - Define safe electronic data handling policies
- Don't forget any paper 'systems'
- Choose the right digital solution(s)

GDPR training

There are a limited number certified GDPR Practitioners in the UK, and they cover all industry sectors. The wealthier sectors, such as financial and professional services, will be snapping these up at increasing day rates.

If you can't find or afford a certified practitioner, there are DPIA Workshops run by the Government. They cost £495 per day and are currently only running in London. However, there are many third parties running GDPR training courses – simply Google 'GDPR training'.

If your organisation is fully compliant with the Data Protection Act, then the first step would be to document how data is managed.

Digital solutions

There is a shortcut if your data is managed by a third party, and the data processing is managed by the third party. You are still responsible for ensuring compliance, but you could ask the third party to document how they manage GDPR compliance.

The simplest example of how this shortcut works is where you are using a fully hosted (cloud) system and the supplier provides a document on how their infrastructure meets GDPR regulations.

The first step to be taken could be to identify all your current computer systems and ask the suppliers how you can meet GDPR regulations – at least this will give a list of work to be done, although don't forget any paper-based systems.

Why are care providers choosing to go digital?

It is proven that care providers who have replaced traditional paper records with digital solutions save time on administration, giving them more time to spend with service users. However, despite numerous benefits, some people are apprehensive about adopting a computerised system due to a perceived lack of security. Yet the right software solution is safer than paper and will enable you to comply with GDPR. With GDPR it makes more sense than ever to adopt a paperless strategy.

Paper is not secure and can lead to data breaches

The GDPR is described by the ICO as an evolution in data protection, not a revolution. If your organisation is fully compliant with the Data Protection Act, then the first step to comply with the new provisions would be to document how data is managed. Yet the new provisions mean that paper is likely to be an insecure form of holding records.

Under the GPDR regulation, it is necessary to know exactly what personal data is held, to evidence why that data is held, and to be able to remove personally identifiable information if requested due to 'the right to be forgotten'. If you can't find information easily in paper documents, it will be extremely difficult to comply with the GDPR. Keeping manual records of who has had access to documentation, the additional burden of documenting why certain information personally identifiable information is held and searching to ensure that all records are removed when requested, will only add to the already huge burden of documentation that care providers shoulder.

Additionally, the retrieval of information itself is necessary under the new regulation and will be burdensome for care providers. Manually searching through folders and files, potentially in cumbersome archives held elsewhere to retrieve the information you need is incredibly time consuming and costly. Having multiple copies of documentation can be dangerous, as it is hard to know if all records are removed, or whether other people hold copies of that information.

Furthermore, it is nearly impossible to track who has had access to the information. Paper records are extremely easy to duplicate on a photocopier, printer, easy to transport outside of a building and easy to dispose of in an insecure way. Care providers can easily expose themselves to data breaches due to a lack of document control simply from using paper to document sensitive information on.

Digital care records are secure and provide better quality of care

In November 2017, CQC updated their key lines of enquiry (KLOE) to encourage providers to embrace digital technology to improve the quality of care. CQC's support for digital technology is motivated by innovative care providers who have proven the benefits of going paperless.

Using electronic evidence of care to create digital care records, care providers can control who has access to records and keep them secure. Digital records are easily searchable, even if that information is archived. Furthermore, records that are accessed or stored in multiple places can be discovered quickly and removed efficiently if necessary.

Not only are documents more secure if stored digitally, but electronic evidence of care produces more valuable care records and enables care staff to provide better care. Using electronic evidence of care delivery, carers and nurses have all the information they need at their fingertips and they can capture comprehensive information quickly and easily. This increases the quality and quantity of real-time, accurate and person-centred information. The quality, quantity and accessibility of digital records enables care homes to provide care that is safe, effective, caring, responsive and well-led care, and reduce safeguarding alerts.

Other benefits of digital care records include a Relatives Gateway, an online portal to keep residents and relatives in touch. The Relatives Gateway enables a greater involvement of a person's social network, promoting inclusive and transparent care. Keeping families in touch with residents' care increases the care providers transparency and openness and builds relatives' trust with the care provider.

How we can help with GDPR compliance

Our range of Mobile Care Monitoring (MCM) products provide a comprehensive evidence of care, electronic care planning and reporting system for social care providers. MCM ensures that you can control the privacy of care records and we help you to meet the data processing requirements of GDPR.

Using MCM you are the data controllers and in full control of information, but we would process information on your behalf. Our software solution doesn't take away your responsibility for ensuring compliance, but we would help you to manage compliance through the following ways:

Investing in infrastructure

We have invested in the best infrastructure for MCM. We use tried and trusted Microsoft Azure, a cloud computing service created by Microsoft. Microsoft Azure's secure, tested cloud hosting infrastructure complies with all the EU privacy laws.

Managed system

We manage backups and security for our customers. The price you pay for MCM includes the software, but also maintenance of the software: the servers, performance, security, disaster recovery and upgrades.

Encryption

All data is encrypted to ensure secure data transfer. Encryption does not prevent interference, but stops would-be interceptors being able to understand the data.

Privacy Policy

Our privacy policy is available within MCM to all users with access rights.

GDPR statement of data held and reason to process

We provide documentation on how our infrastructure meets GDPR regulations and a statement of intent and reason to process data. This will be in a template form for care providers so you can edit the information for your service.

Fully auditable access to records

To comply with the GDPR, care providers will need to be able to show documentation for the reason for processing personally identifiable information and show who has accessed that information. To give the thorough information about who has had access to records, MCM will track each screen, showing who has had access to data and when. We are reviewing how best to help providers prove who has accessed records, for instance various ways to digitally track printouts from the system.

Frequent Penetration testing

A penetration test (pen-test) evaluates the security of an IT infrastructure by trying to exploit vulnerabilities. We arrange frequent external penetration tests to ensure MCM is as secure as possible and the system is protected from any cyber-attacks or from people trying to intercept data. Our pen-tests are externally approved, and we receive a certificate along with the results to document our security testing.

Photos on secure photostream

A valuable feature of digital care records is the ability to take photos of service users at the point of care on mobile devices. Photographs quickly give visual real-time evidence on a body map, support wound care progression records, and capture special moments that can be shared with families though the Relatives Gateway.

If photos are stored on the mobile device's own gallery, other people could access and view sensitive images on the device if it was misplaced. Furthermore, the images would be held in the device's shared online gallery that might be outside the EU.

To solve this potential security risk, MCM has a secure 'photostream' that enables staff to take photos of the people they support through the Care App. Once saved, these photos cannot be displayed from the device, but are automatically synchronised with a gallery in

the care monitoring side of the system. Staff with the correct usage rights can then attach these images to service users' wound care records, share with relatives, or use as an updated profile picture. The photostream is a secure facility to document or share valuable photographs, to involve families in care, or as supporting documentation for medical records. If photos haven't been attached to service user records within 28 days they are automatically deleted, to ensure the care provider is not storing images unnecessarily.

Mobile Device Management

We manage the mobile devices that our customers use the MCM software on. Mobile Device Management gives us the ability to control the information that a mobile device can access.

With Mobile Device Management we:

- Lock down devices so staff can't access any internet browsers. This ensures that they can't access any websites that may expose the system to being hacked. It has the additional benefit of ensuring that staff use the devices purely as a tool to record care.
- Wipe devices remotely so information can't get in to the wrong hands if the device is lost or stolen.
- Ensure that only enrolled devices can access the data.
- If requested, can further lock down devices so they can only be used on internal IP address. This means that the devices wouldn't work outside of the care provider's Wi-Fi network.

Secure data management

Under the GDPR regulation, care providers shouldn't hold personally identifiable information unnecessarily. This means that services must dispose of service users' records after a period. Identifying records that should no longer be stored is time-consuming and costly, and laborious to dispose of them securely. MCM would identify care providers' records that were no longer necessary for you to keep, automatically alert you, and enable you to dispose of them securely with a few clicks of a button. Not only does this save a huge amount of time, but ensures that data management is always up-to-date.

The future

There is no hiding from GDPR. Action needs to be taken urgently, but don't panic. Start by speaking to your system providers, consider what data you hold and how it is processed. Make sure all staff are aware of their responsibilities and start to train them in GDPR. It will feel like a lot of work, but the penalty for non-compliance is huge and the sector can't afford another cost.

To find out more about GDPR compliance:

- Get in touch on 01483 604108 or email care@personcentredsoftware.com or contact us www.personcentredsoftware.com to find out how we can help your service.

References ICO: https://ico.org.uk/for-organisations/data-protection-reform/