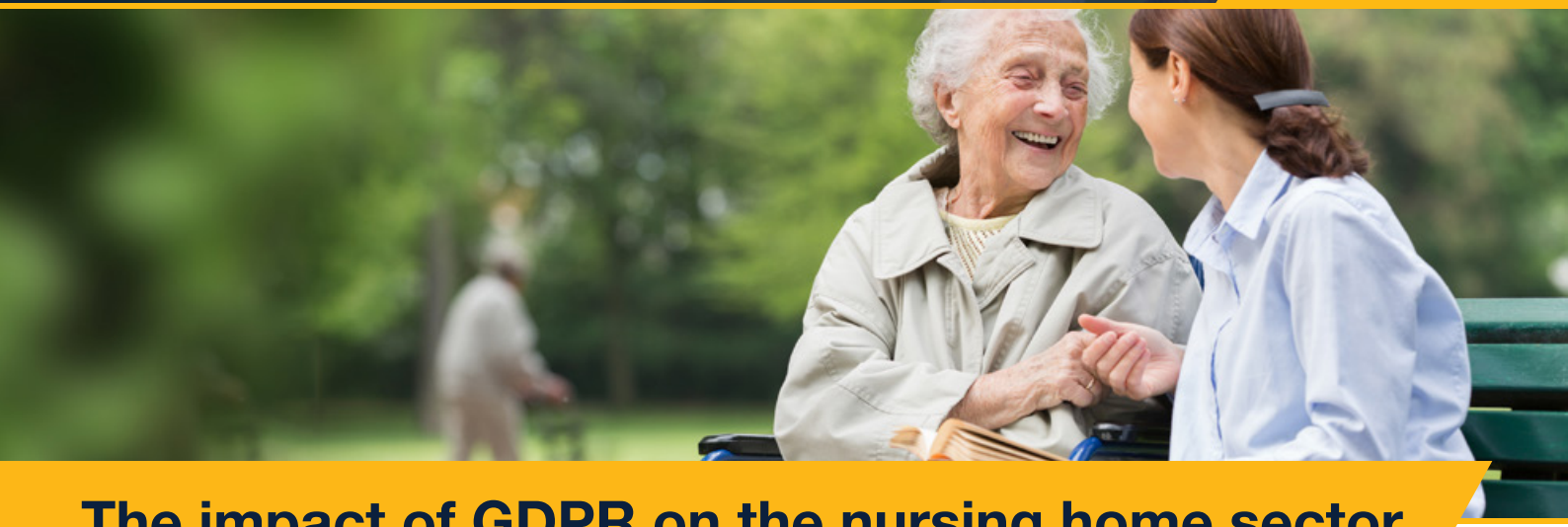
Crowe Horwath

Smart decisions.
Lasting value.



The impact of GDPR on the nursing home sector

GDPR and the nursing home sector

When it comes to data protection, there are few sectors as vulnerable to threats as the nursing home sector with the volume of personal, medical and financial information being processed on a daily basis.

With the enforcement deadline for the GDPR looming closer, it is imperative that the nursing home sector upgrade their data protection processes, or they face the risk of large financial penalties and potential severe reputational damage.

The penalties for not complying with GDPR are large, at a financial cost of up to €20 million or 4 per cent of worldwide annual turnover (whichever is greater), not to mention the potential reputational cost to an organisation in this sector. However, these possible losses can be avoided if the sector leaves enough time to efficiently adapt to the regulation.

What is GDPR?

GDPR is a regulation to strengthen and unify data protection for individuals within the European Union. It was adopted in May 2016 and following a two-year implementation period will come into force on 25 May 2018. The legislation brings in a large number of changes, meaning that the level of effort involved in preparing for GDPR compliance is significant.

Capturing and using personal data

Personal data must be collected for specified explicit and legitimate purposes. Data cannot be further processed in a conflicting manner with the purposes outlined initially. The nursing home sector must ensure residents and employees, for example, are aware of the particular uses of their data.

Your 5-stage plan to preparing for GDPR

It is essential that your organisation creates awareness and has full buy-in from all employees that process and retain data in the organisation.

As a result of GDPR there may be changes in procedures or systems required, so adequate resources should be set aside to update existing policies and procedures to ensure compliance, and staff should have appropriate training for the ongoing maintenance of GDPR compliance. All relevant employees should not only be aware of GDPR, but they should fully understand and appreciate its impact.

It is important that the nursing home sector devise and implement a plan now to ensure compliance with GDPR before its introduction in May 2018. Below is a five-stage plan to GDPR compliance.

Stage 1 – Identification of responsible individuals

Nursing home management should first identify the relevant individuals who will implement and monitor the data protection plan in the organisation now and going forward. In accordance with the guidance issued by the Health Information and Quality Authority (HIQA) in October 2017, a service provider who processes personal health information must appoint a suitable qualified and experienced Data Protection Officer (DPO).

Stage 2 – Privacy Impact Assessment (PIA) process

In accordance with HIQA's published guidance, a service provider who processes personal health information must conduct a data Privacy Impact Assessment. The PIA serves as an 'early warning' for detecting potential privacy risks and involves the following key stages:

- Stage 1 – Threshold assessment
- Stage 2 – Identify the privacy risks
- Stage 3 – Address risks and evaluate privacy solutions
- Stage 4 – Produce the PIA report
- Stage 5 – Incorporate the PIA outcomes into the project plan

Stage 3 – Policies and procedures review

Nursing home organisations will need to review all current data protection policies such as their privacy policy, SAR (subject access request) policy, retention policy and other policies like shredding and breach management policy. Their policies relating to third party data contractors should also be reviewed.

Stage 4 – Training

Staff awareness and education should be a key concern for organisations implementing GDPR. Engaging staff in relevant training is critical to your plan's success. A staff awareness programme should be an ongoing process that begins at induction and is reinforced regularly throughout the year and/or whenever staff-related data protection incidents occur.

Stage 5 – Ongoing review and monitoring

Maintaining GDPR awareness with staff is an ongoing process. The nursing home organisation should provide regular refresher training for all staff to ensure an awareness culture exists to protect against possible breaches. Management should incorporate data privacy into operational training such as induction, HR and security, and conduct regular access request drills to ensure efficiency with 'Right to Seek' requests.

Other considerations

Change to right of access to personal data under GDPR

Under existing Data Protection Acts any individual can write to an organisation and request personal information for a fee of €6.35 and the onus is on the organisation to furnish this data within 40 days. This personal data can relate to both electronic and physical forms and would identify an individual by their personal information such as name, address, dietary, medical conditions, etc. Under GDPR these 'Right to Seek' personal data requests will now be free of charge.

In the run up to the effective date of 25 May 2018, the Data Commissioner's Office will be running a public awareness campaign about a consumer's 'Right to Seek' their personal data. As a result of that campaign, and because these requests are now free, we anticipate there may be an increase in individuals requesting their personal data. Also under the new regulation organisations will need to comply within the shorter period of one month or be subject to a breach of the regulation.

Third party partners

The nursing home sector should put their third-party partners under greater scrutiny, as they can often prove to be a business's vulnerable point in terms of data protection. A major change due to GDPR is that data processors are captured by the regulations as well as data controllers. This means that if a nursing home, as a data controller, is outsourcing the processing of data to a third party who is not complying with GDPR regulations, the nursing home and the third party processor can be held jointly responsible if a breach occurs.

Next steps

It is important that nursing home organisations act now to fully access the true impact of the new regulations. The GDPR team at Crowe Horwath can help devise and implement a plan to ensure compliance in advance of the May 2018 deadline. If you would like to find out more about how we can help you, contact Simone Kennedy and Catherine Rogers of our risk consulting team.

About Us

Established in 1941, Crowe Horwath is a leading accountancy and business advisory firm in Ireland. Throughout our 75-year history, we have developed an unrivalled understanding of the Irish business environment and built a national reputation in auditing, tax and business consultancy.

We work with a variety of clients across commercial and public sectors. Our services include Audit & Assurance, Tax, Corporate Insolvency & Recovery, Corporate Finance, Consultancy, and Outsourcing.

We are also independent members of the eighth-largest accountancy network in the world, with colleagues in over 750 offices across 130 countries. Through this global reach we are able to offer clients a seamless service when trading internationally.

Contact

Crowe Horwath Bastow Charleton
Marine House
Clanwilliam Place
Dublin 2

Tel: +353 1 448 2200
www.crowehorwath.ie

Simone Kennedy, Internal Audit
Direct Dial: +353 1 448 2265
simone.kennedy@crowehorwath.ie

Catherine Rogers, Consulting
Direct Dial: +353 1 448 2321
catherine.rogers@crowehorwath.ie