GDPR – Employee Q&A

What is GDPR?

GDPR stands for 'General Data Protection Regulation'. It's a new EU Regulation which will still apply after Brexit.

Why is it important?

It represents the biggest shake-up in data protection law for more than 20 years. It applies to every aspect of our organisation where we control or process personal data – whether that's in our IT, Finance, HR systems or elsewhere. Personal data is anything which identifies an individual and it's important to ensure personal data is used in the right way, kept safe and secure and that people understand how their data is being used.

Is GDPR the same as Information Governance?

No – but the two are closely related. Information Governance in an NHS setting, such as Viapath, is concerned with protecting the confidentiality of Patient Identifiable Data (PID) on behalf of patients. GDPR is about the data protection rights of everyone.

How we handle patient data is an important part of the GDPR project. All employees will need to undergo GDPR training in addition to the current mandatory IG training.

Why does it matter to me?

Every day at Viapath we process patient data to carry out tests and provide test results to our customers. As employees, our own personal data is also held in our employee records. We should all care about what happens to personal data and we all have a role to play in ensuring Viapath is compliant with the new Regulation. There are huge fines of up to 4% of turnover for non-compliance.

How can I help?

Keep all personal data secure! You should do this by:

- Maintaining a clear desk
- Locking hard copies of documents in secure storage facilities
- Locking your computer screen when away from your desk

Recent communications talk about a data clean up, what do I need to do?

The data 'clean up' will mainly affect HR and anyone involved in recruitment. We expect this might take a short while to do and it needs to be complete by the end of June 2018.

You will need to confirm that you have undertaken this exercise as part of your Data Protection training.

PLEASE TAKE THE FOLLOWING STEPS:

- Delete any CVs, bios or interview notes in your email folders or on your computer which are more than 12 months old. You DO NOT need to look in email archives (.pst) files, in your Outlook calendar, in shared email boxes, shared drives or SharePoint.
- Delete any 'non-master' files (i.e. copies) of employee data which are more than 12 months old – this is most likely to be in the form of spreadsheets or other manually populated documents retained on your computer.
- Dispose of any hard copies of the above in the confidential waste bins

YOU DO NOT NEED TO DELETE:

- Patient data
- Contact details of individuals at customers or suppliers

I am a people manager and I keep records of things like sickness/doctors notes, appraisal documents etc and other personal details for my team on my computer or in a locked filing cabinet – can I continue to do so?

Ideally you would keep only the information you need to manage your team and store it electronically in a password protected folder in Sharepoint or on a shared drive. You can retain paper copies provided they're kept securely (e.g. a locked filing cabinet) but bear in mind that you should not retain information for any longer than necessary.

Please therefore only keep what you need to do your role and if someone has left your team, ensure relevant documents are passed to HR for storing on their file including scanning and sending over any paper copies. Please also consider how, going forward, MyHR can help you to avoid storing information separately.

Where can I get help?

If you have any questions please contact: askus@viapath.co.uk