

Heart Networks UK Limited and GDPR

(General Data Protection Regulation)

As an organisation, we take issues of information governance and data privacy very seriously. They are at the heart of what we do.

What is GDPR?

Each member state in the EU operates under the current 1995 Data Protection Regulation and has its own national laws. In the UK, the current Data Protection Act 1998 sets out how your personal information can be used. The General Data Protection Regulation (GDPR) changes how data can be used and is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen data protection. Companies who hold or process data need to be compliant with the GDPR regulation by May 2018.

What is Heart Networks UK Limited doing about this?

As an organisation, we take issues of information governance and data privacy very seriously and have them at the heart of what we do. Some of the things we are doing to ensure compliance with the new regulation are sensitive, but we can confirm that we have created a project plan that we are busy working through to help ensure that we are compliant.

We are happy to share with you, a high level overview of some of the steps we are taking, or are planning to take, in relation to the forthcoming changes in data privacy law.

Raising awareness

One of the key steps for any organisation to take is to raise awareness of the changes so that people across the business are alive to the issues.

- We are raising awareness of information governance issues across the Organisation, for example, through the delivery of bespoke training, through training modules, through use of our internal newsletters and, going forward, through the revised IG toolkit made available by NHS Digital.
- We are revisiting all our data related policies, including arrangements for compulsory breach notification so that staff know who to contact should an incident arise (taking into account the obligation to do so without 'undue delay').
- We will engage with sector specific bodies, active in setting standards, (e.g. the Information Governance Alliance) so that we are aware of any relevant codes of practice.

- We are engaging on an ongoing basis with our partner organisations to identify those elements of the GDPR which we believe may be impacted going forward.
- We are revisiting our Data Protection impact assessment process to ensure that PIA's are undertaken as required.

Review of data security

We recognise the need to meet the integrity and confidentiality principles under the GDPR and to this end, we are therefore reviewing our:

- data security standards
- data breach, storage and destruction policies and management
- data security action plan

To ensure that they are fit for purpose.

Data protection officer

We have appointed a Data Protection Officer (DPO) with overall responsibility for compliance within the Organisation.

Policy and contract review

We are presently reviewing (and updating as appropriate) our:

- data privacy related policies and procedures
- data sharing agreements (and process)
- fair processing notices ('privacy policies') and website terms

To ensure they are fit for purpose.

We will review and revise as appropriate to ensure we meet and reflect all the requirements of the new regime.