IT and Data Services
Provide
900 The Crescent
Colchester
Essex
CO4 9YQ

0300 303 9999
Provide.infogov@nhs.net

15 May 2018

Re: General Data Protection Regulation ((EU) 2016/679)

New data protection legislation is due to come into force on 25 May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data.

Provide welcomes the new data protection legislation and acknowledges that, as sensitive data as defined by the new data protection legislation is currently shared between ourselves, we would like to ensure that this legislation is recognised going forwards and share with you the work we have been undertaking to prepare for these changes.

Background

Provide CIC, as a provider of NHS and Local Authority community services complies with all NHS statutory guidance, including the Department of Health's Confidentiality: NHS Code of Conduct, Information Security Management Code of Practice and records management policies.

Provide is registered as a Data Controller with the Information Commissioner's Office. Our notification number is Z2604172.

Use of the NHS Digital Information Governance (IG) Toolkit allows us to effectively assess ourselves against the standards required to protect all patient related information.

The last submission of the IG Toolkit took place in March 2018. We achieved 79%, which is an improvement from our last submission and has continued the trend of a year-on-year improvement in our IG assurance.

As well as the assurance provided through the IG Toolkit, the organisation also obtained ISO 27001 accreditation for its IT and Data Services in January 2018. ISO 27001 is recognised worldwide as the standard for information security management. To gain the ISO 27001 award, the organisation proved that we could not only prevent but defend against potential data system vulnerabilities.

This achievement was due to our comprehensive suite of information security controls and the management system we introduced to ensure these controls remain efficient and continue to meet our customers' needs.

This standard will also help to demonstrate compliance with the new General Data Protection Regulations (GDPR) which has formed an integral part of the IG assurance programme over the past year.

Provide is very pleased to have been accredited under The Cyber Essentials Plus scheme. Developed by the UK Government and industry, it defines a set of controls which, when implemented, give assurance that the organisation meets a standard of protection from the most prevalent forms of threats coming from the internet. In particular, it focuses on threats which require low levels of attacker skill, and which are widely available online. A recommendation from the National Data Guardian's Data Security, Opt and Consent Review was that all health and social care organisations should be accredited to the Cyber Essentials Scheme.

Preparations
Provide CIC engaged with a third party consultancy company, RiskX in July of last year to perform a review of our current systems and business processes against GDPR and to effectively audit our current practices. They provided us with a Gap Analysis Report, including the key activities that we needed to complete in order to achieve compliance with the new regulations.

The outputs of the report formed the basis of our action plan for preparing for GDPR. Our preparation has included:

User awareness: Information Governance Refresher Training has been updated to include updates pertaining to GDPR. All staff are required to undertake IG training on an annual basis. We have been cascading updates out through our network of Information Champions as well as through our weekly newsletter and our Metacompliance policy delivery system. We have also been trialling an Information Governance Board Game which we have been making available to teams to use at team meetings.

Register of processing activities: The Information Governance Team have been engaging with and visiting all Provide services to map out the information that they hold, how they hold it, what they process it for, as well as the legal basis for processing and who they share it with, including how the security of the information is maintained during transfer. This has formed the basis of our Information Asset Register. We are currently in the process of uploading this information to our Information Asset Register system, 'Flowz' that the organisation has invested in to maintain this information over time.

Communicating privacy information: We have reviewed our suite of privacy notices and have updated these in light of the new requirements of GDPR. Provide is taking a layered approach to providing privacy information which includes providing information on its websites and providing information in printed leaflet form. The aim has been to ensure that information is provided to patients which is concise, transparent, intelligible and easily accessible and we are currently developing an easy read guide for children and those with special requirements.

Appointment of a Data Protection Officer (DPO): Provide, in conjunction with Medway Community Healthcare and Your Healthcare, has appointed a DPO, Richard Bradley. Richard has previously worked in Information Governance with the Nursing and Midwifery Council (NMC).

Privacy by design: We have trialled a methodology for the completion of Data Protection Impact Assessments and are completing these for any projects, initiatives or data sharing where it "is likely to result in a high risk to the rights and freedoms of individuals".

Subject access requests: We have reviewed our processes for responding to access requests by data subjects. We have streamlined our processes to ensure compliance with any requests within one calendar month and free of charge as the new regulations stipulate. We can now comply with requests electronically by sending records by secure encrypted email where requested. Our new processes went live on 1 May.

Breach detection: The organisation has invested heavily in its IT infrastructure to ensure the confidentiality, integrity and availability of the data that we hold and process. We have invested in a system called Varonis which is a data security platform that protects our file servers from cyberattacks and insider threats. The system analyses the behaviour of the people and machines that access our data, alerts on misbehaviour, and enforces a least privilege model with regards to access rights. It also identifies where our most sensitive data is held (GDPR Patterns) and alerts us and takes automatic action if there has been any attempted processing by unauthorised persons. We have reviewed our incident reporting processes to ensure that they are fit for purpose when the new regulations come into force.

Supplier and third party assurance: Our contracts team have been engaging with suppliers and companies that we contract with that process our data to ensure that they are compliant with the new regulations and including variations to all applicable contracts.

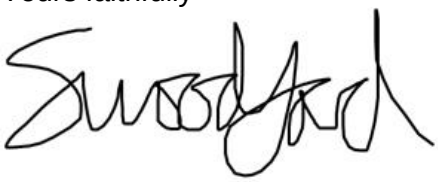
Next Steps

Provide CIC recognises the need for continual improvement and that the new regulations extend beyond 25 May 2018. Therefore work is continuing in the following areas:

- Updating Information Sharing Agreements (ISAs) we have in place with partners and third parties.
- Updating our Information Governance Policy Suite to ensure that they are compliant with the new regulations.
- Embedding the new Information Asset Register System across all of our services.
- Continued cascading awareness materials to staff regarding key changes.

I hope that you find this update helpful. If you require any further information, please contact myself or my team who will be happy to help (provide.infogov@nhs.net)

Yours faithfully



Steve Woodford
Information Governance and IT Projects Manager