GDPR Assurance Statement

The General Data Protection regulation (GDPR), coming into force on the 25th May 2018, alongside the Data Protection Bill replaces the current Data Protection Legislation . Pinnacle wishes to assure all of our clients that we are working hard on ensuring compliance in all areas of our business.

Within this statement we want to highlight to our customers the measures we have put in place to ensure compliance with the GDPR where we hold or process personal data on your behalf.

Data Protection Officer

Pinnacle has designated a Data Protection Officer – Pamela Bowes dpo@phpartnership.com

Pamela is a certified EUGDPR Practitioner and is taking full responsibility for all matters relating to data protection and GDPR compliance. The DPO will ensure that we are accountable and transparent to the supervisory authorities.

Security and Business Continuity Measures

Pinnacle works to ensure the confidentiality, integrity and availability of the personal data we store or process. We maintain appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

In demonstration of this, we have achieved and maintain the following standards:

NHS IG Toolkit Level 3

ISO27001:2017 certification for Information Security Management Systems

Cyber Essential Plus

Customer and End User Contracts

To adhere to the GDPR requirement, a data controller (our client) must appoint the data processor (Pinnacle) formally in writing, in our case, in the form of our Service Level Agreement and End User Licence Agreement. The document must state that the personal data is processed only on documented instructions from the controller or to meet the requirements of EU or UK law. We will be reviewing all of our agreements to ensure compliance. This will ensure that relevant wordings are in place to cover aspects such as nature and purpose of the processing, the types of data processed and the obligations and rights of the controller.

Data Breaches

Under GDPR, we must notify any data breach to the controller without undue delay. Pinnacle therefore has processes and procedures in place for identifying, reviewing and promptly reporting data breaches to the relevant controller and assisting with any remedial action or reporting required.

We would, however, stress that we have comprehensive technical and organisational security measures in place to mitigate against a data breach.

Data Subject Rights

Under GDPR there are significant enhancements to the rights that individuals enjoy with regards their personal data. Although there is a legal requirement for health data to be recorded and for those records to be kept for regulated time periods, Pinnacle can work with Clients in order to determine how best to facilitate:

Handling Data Subject Access Requests

Pinnacle Systems allow Clients to access information to answer these requests but are also willing to assist where required.

Retention Periods

Data is retained according to the current guidelines or the explicit instructions of the relevant Data Controller.

Please consult the detailed retention schedule (appendix 3) in the link below https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016)

Secure Erasure / Destruction of Personal Data

Pinnacle has procedures in place for the secure return/archiving/destruction of data when this is required.