To keep your data safe, David Barber (OH) Ltd use a system called Orchid Live. This system is confidential and allows medical data and reports to be delivered to named people only who have been given access to the system.

Orchid Live provide this Statement of Compliance.

General Data Protection Regulation (GDPR)
**OrchidLive Overview**

**Introduction**

The new EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 (including in the UK regardless of its decision to leave the EU) and will impact every organisation which holds or processes personal data. It will introduce new responsibilities, including the need to demonstrate compliance, more stringent enforcement and substantially increased penalties than the current Data Protection Act (DPA) which it will supersede.

OrchidLive is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data in accordance with accepted standards including ISO 27001. The company will comply with applicable GDPR regulations when they take effect in 2018, including as a data processor, while also working closely with our customers and partners to meet contractual obligations for our procedures, products and services.

The company has two main areas of focus in preparing for GDPR overseen by an internal cross-functional team:

1. Building on existing security and business continuity management systems and certifications, including ISO 27001, to ensure our own compliance
2. Product programmes to support compliance for users of our software applications including solutions to streamline the process and drive greater efficiency

It is important to recognise that compliance is a shared responsibility and all organisations will need to adapt business processes and data management practices.

1. **Compliance**

OrchidLive has a robust ISO-based Management System (ISMS) and in order to ensure compliance will implement additional or augmented company-wide controls to meet GDPR requirements within the ISMS using internal and external advisors. Led by our Data Processing Officer, updated information security policies and procedures will build on existing management systems (including ISO 27001) and the foundation of our Information Control and Classification policy, informed by gap analysis and data protection risk assessments and supported by communication and training programmes.

Compliance will be supported by a review of existing contracts with data controllers, the use of sub-contractors and any data export arrangements.

OrchidLive’s Data Protection Officer will inform, advise and monitor compliance. The company will implement tools as appropriate that support the process, provide necessary security and ongoing delivery of objectives.

In many areas the hosted services provided by OrchidLive already conform. As data processor, the company is undertaking risk assessments to include more detailed consideration of the data types we hold and a data protection impact analysis of personal information stored and processed. Policies such as incident response plans and backup data retention will be reviewed and updated.

**2.     OrchidLive software application**

OrchidLive’s software application is used to provide efficient and high quality services. As such the company is committed to providing technology solutions to support customers’ GDPR obligations, whether through standard features or added value solutions or toolkits.

All organisations will need to be confident, for example, that personal and transactional data can be located and anonymised or erased, in order to respond to requests to delete, rectify, transfer, access or restrict the processing of data.

Customers should contact their account manager to understand what features are available to enable this, from data cleansing and subject access reports to specific data retrieval and disposal tools which create efficiencies by allowing organisations to locate, anonymise and remove data with minimal administrative effort and to enable a quick and efficient response to information requests.