Penn Hill Dental Practice

Information Governance, Data Protection & Security Policy

1. **Introduction**

   Information is a vital asset, both in terms of clinical management of individual patients & the efficient management of services & resources. It plays a key part in clinical governance, service planning & performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2. **Purpose of the policy**

   This Information Governance policy provides an overview of the practice's approach to information governance ; a guide to the procedures in use; and details about the IG management structures within the dental practice.

3. **The practice's approach to Information Governance**

   Penn Hill Dental Practice undertakes to implement IG effectively and ensures the following:

   - Information will be protected against unauthorized access
   - Confidentiality of information will be assured
   - Integrity of information will be maintained
   - Information will be supported by the highest quality data
   - Regulatory and legislative requirements will be met
   - Business continuity plans are produced, maintained & tested.
   - Information governance training available to all staff as necessary to their role.
   - All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4. **Procedures in use in the Practice**

   This IG policy is underpinned by the following procedures:

   - **Records management procedure** that sets out how patients dental records will be created, used, stored & disposed of
   - **Access control procedure** that sets out procedures for the management of access to computer based information systems
   - **Information handling procedure** sets out procedures around the transfer of confidential information
   - **Incident management procedure** sets out the procedures for managing and reporting information incidents

- **Business continuity plan** sets out procedures in the event of a security failure or disaster affecting computer systems.

5. **Staff guidance**

   Staff compliance with the procedures is supported by the following guidance material:

   - **Records management:** guidelines on good record keeping
   - **Staff confidentiality code of conduct:** sets out the required standards to maintain the confidentiality of patient information; obligations around the disclosure of information and appropriately obtaining patient consent;
   - **Access control:** guidelines on the appropriate use of computer systems
   - **Information handling:** guidelines on the secure use of patient information
   - **Using mobile computing devices:** guidelines on maintaining confidentiality and security when working with portable or removable computer equipment
   - **Information incidents:** guidelines on identifying and reporting information incidents.

6. **Responsibilities & Accountabilities**

   The designated **Information Governance Lead** for the practice is Gary Irvine.

   The key responsibilities of the lead are:

   - Developing & implementing IG procedures & processes for the practice
   - Raising awareness & providing advice & guidelines about IG to all staff
   - Ensuring that patient data is kept secure & that all data flows, internal and external are periodically checked against the Caldicott Principles.
   - Ensuring any training made available is taken up
   - Monitoring information handling in the practice to ensure compliance with law, guidance, and practice procedures.
   - Ensuring patients are appropriately informed about the practices information handling activities.

The day to day responsibilities for providing guidance to staff will be undertaken by Gary Irvine.

The **owner** of the practice is responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework.

All **staff,** whether permanent, temporary or contracted, are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

7. **Approval**

   This policy has been approved by the undersigned & is reviewed annually.

   Gary Irvine 17/5/21 Next review on/before 17/5/22