Audit Tool : Data Protection

Standard: Appropriate standards and measures are in place to ensure the legal collection, usage and protection of patient information in accordance with the Data Protection Acts of 1988 and 2003.

Date: _____ Surgery/Practice: _____

Auditor (print name): _____

Compliance Officer: _____ Job title: _____

Rule	**Data Protection Rules**		
1	Is personal data obtained and processed fairly?		
2	Is personal data kept for one or more specified, explicit and lawful purpose?		
3	Is personal data used and disclosed in ways compatible with the specified, explicit, lawful purposes?		
4	Is personal data kept safe and secure?		
5	Is retained personal data accurate, complete and up-to-date?		
6	Is personal data adequate, relevant and not excessive for the purpose or purposes?		
7	Is personal data retained for no longer than is necessary for the purpose or purposes?		
8	Is there a clear procedure in place to provide a copy of his/her personal data to that individual, on request?		

All questions must be answered **Yes** to achieve a **Pass** in each section, except where otherwise indicated.

	Principle: Obtain and process personal data fairly.	**Yes**	**No**
1.1	Is the data collection process explained to a patient? • What information is being collected • Why is the information being collected • Who within the practice has access to the information • Who outside the practice may have access to the information		
1.2	Is a patient aware of the consequences of not providing valid information?		
1.3	Is a patient aware of his/her rights? • Access to personal data • Rectification of personal data		
1.4	Is patient aware of how his/her information is stored?		
Optional	Is a patient provided with a practice *Patient Privacy Statement*?		

	Principle: Keep personal data only for one or more specified, explicit and lawful purposes.	**Yes**	**No**
2.1	Is the data collected solely for the dental care of a patient?		
2.2	Is a patient aware of any other use which may be made of his/her personal data?		

2.2	Is valid consent received prior to using data for purposes other than providing dental care?		
2.3	Is a patient aware of the different types of data collected and retained? • Personal details • Medical history • Dental record • Financial information		
2.4	Is a patient aware that his/her personal data may be used other than for dental care? • Report to dental insurance company • Medico-legal report • Teaching/lecturing purposes • Continuing professional development • Internal audit • External research • State schemes • Direct marketing		
2.5	If information has been gather for the purpose of direct marketing has the patient's consent been obtained?		
2.6	If electronic mail is used for direct marketing can the recipient UNSUBSCRIBE immediately and for free?		
2.7	Are all disclosures of data legitimate?		

	Principle: Personal data should be used and disclosed in ways which are compatible with the reasons for which it was obtained.	**Yes**	**No**
3.1	Is 'Confidentiality' upheld in accordance with Dental Council Code of Practice (*Section 10, Professional Behaviour and Ethical Conduct, 2012*)?		
3.2	Is patient confidentiality included in staff training?		

3.3	Is access to patient records on a 'need to know' basis? • To a guardian/carer • Within the practice staff • Upon referral to a colleague • Medical healthcare provider		
3.4	Does the transfer of personal data respect the individual's rights? • Consent to transfer • Accuracy of data transferred • Confidentiality • Security of data transfer		
3.5	Are the individual's rights respected whenever data is transferred? • When a patient transfers to another healthcare professional within the practice • When a patient transfers to another practice • Upon retirement, death or closure of a practice • Sale of a dental practice		
Optional	Is there a professional confidentiality code within the practice?		
Optional	Does the practice have a means of auditing when patient information has been accessed and by whom?		

	Principle: Keep personal data safe and secure.	**Yes**	**No**
4.1	Who, in the practice, is responsible for the security of data? Name:_____ Job title:_____		
4.2	Is access to patient records on a 'need to know' basis?		
4.3	Is data protection included in staff training?		

4.4	Is the premises locked and alarmed when not in use?		
4.5	Is a fax machine used to transmit personal data? (If 'Yes' please answer 4.6. If 'No' please go to 4.7)		
4.6	Is the fax machine in a secure area not accessible to the public?		
4.7	Are patient records kept manually? (If 'Yes' please answer 4.8, 4.9. If 'No' please go to 4.10)		
4.8	Is access to the manual record system barred to the public?		
4.9	Is the filing room/filing cabinet(s) locked when not in use?		
4.10	Are patient records kept on computer or any other form of electronic storage? (If 'Yes' please answer the remaining questions as indicated. If 'No' please go to 4.30)		
4.11	Is the relevant staff trained in the appropriate and secure use of the practice computer systems and the internet?		
4.12	Are screens/monitors out of view of the public?		
4.13	Does each workstation have a password-protected screensaver?		
4.14	Are CDs, DVDs or disks kept in locked drawers?		
4.15	Is all software legally owned by the practice?		
4.16	Is the practice software password-protected?		
4.17	Is the operating system updated regularly? • Automatically • Manually • By the maintenance provider		

4.18	Is anti-virus/internet security software, compatible with your operating system, installed and running?		
4.19	Is the anti-virus/internet security software regularly updated?		
4.20	Are regular full-system scans undertaken?		
4.21	Are servers housed in secure, appropriate conditions?		
4.22	Is personal data stored on portable devices (laptops, smartphones, tablets, external drives or any other form of electronic storage)? (If 'Yes' please answer 4.23 – 4.26. If 'No' go to 4.27)		
4.23	Are all portable devices stored securely when not in use?		
4.24	Are all portable devices password protected?		
4.25	Is all personal data stored on mobile devices encrypted?		
4.26	Is a name and contact information affixed to all portable devices in case of loss?		
4.27	Are all patient records backed up daily?		
4.28	Is the data controller satisfied that the back-up system is secure?		
4.29	Is there a contract in place delineating the responsibilities for security of data*, present and into the future, and the retrieval of data (disaster recovery measures) for all online backup services? (*Equivalent to those imposed on the data controller under the Data Protection Acts)		
4.30	Is there a written practice policy on breach management?		
4.31	Who, in the practice, is responsible for dealing with a breach incident? Name:_____ Job title: _____		

4.32	In the case of loss/theft of retained personal data is it appropriate to notify persons/authorities? • People about whom personal data was retained • An Garda Síochána • The Data Protection Commissioner		
Optional	Are patients aware of the use of online backup services, e.g. *Patient Privacy Statement*?		
Optional	Is there a written practice policy on the use of emails?		
Optional	Is there a written practice policy on the use of the internet?		
Optional	Is there a written practice policy on the use of fax machines?		

	Principle: Keep personal data accurate, complete and up-to-date.	**Yes**	**No**
5.1	Is personal data updated? • Every visit or • Annually		
5.2	Is the information gathered accurate, complete and contemporaneous?		
5.3	Is the information dated?		
5.4	Is the information comprehensible and legible?		
5.5	Is the information well organised for efficient retrieval?		

	Principle: Ensure that personal data is adequate, relevant and not excessive.	**Yes**	**No**
6.1	Is the data adequate to serve its purpose effectively?		
6.2	Is the data relevant, and not excessive, for its purpose?		
Optional	Is there a written practice policy on the production of effective patient records?		

	Principle: Retain personal data for no longer than is necessary for the specific purpose(s).	**Yes**	**No**
7.1	Is there a practice policy on the retention of personal data? • Patient records • Staff records		
7.2	Does the policy oversee the management of different retention systems? • Manual records • Electronic records		
7.3	Is the destruction of manual records certified?		
7.4	Is the destruction of information stored on hard drives (internal/external), CD, DVD, floppy disc, microfiche or any other form of electronic storage device certified at the time of equipment upgrades?		
7.5	Are the certifications of destruction retained?		

	Principle: Individuals are entitled to a copy of their records.	**Yes**	**No**

8.1	Is there a clear, legally-compliant practice policy re: request to access of personal data?		
8.2	Is there a named person to process access requests? Name: _____ Job Title: _____		
8.3	Does the practice policy comply with the requirements of the Data Protection Acts (1998, 2003)? • Right of Access • Right of rectification/erasure of inaccurate data • Consent obtained for marketing • Right to be removed from direct marketing/mailing list • Right to complain to the Data Protection Commissioner		