Information Governance Compliance in Dental Practice

(Legal and Ethical)

Aims: This article aims to discuss the importance of Information Governance in dental practice. It will outline the key areas that need to be considered to have a consistent approach to information handling and ensure that the practice handles information in line with the relevant laws and meets the standards set out by the General Dental Council.

Objectives: On completion of this verifiable CPD article, the participant will be able to demonstrate, through completion of a questionnaire, the ability to:

- Recognise the relevant UK laws and professional standards governing information governance
- Understand the roles and responsibilities of the practice's information governance lead.
- Identify essential components of an information governance policy.
- Have knowledge of appropriate training requirements for the dental team.
- Understand lawful bases for processing and sharing patient information.
- Be familiar with the UK GDPR and professional standards, including the Caldicott Principles.
- Identify key areas for ensuring information security and confidentiality.
- Have knowledge of incident management and reporting requirements.
- Complete an on-line assessment, scoring over 70%

Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of a dental practice. It plays a key part in clinical governance. It is 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. Dental practices must handle information in line with UK data protection law (UK GDPR and Data Protection Act 2018) and meet standards required by regulators such as the Care Quality Commission (CQC) and professional bodies like the General Dental Council (GDC) [1]

This means that everyone working for or on behalf of the dental practice complies with Information Governance requirements. All members of staff, i.e., employees, permanent or temporary, locums, volunteers, students, and IT support companies;

should have a specific and explicit clause in their contract of employment, volunteer agreement or contract for services (e.g., IT services) stating an obligation to keep personal information confidential. Otherwise, the dental practice may have little or no defence in the event of an accidental or intentional breach by a member of staff or third party. The contract will also provide a formal record that the practice has taken steps to ensure that staff recognise their own responsibility for protecting health and care information. [2]

Effective information governance supports patient safety, continuity of care, and public confidence in dental services.

Professional Responsibility

In dentistry, we have an obligation to be registered with the General Dental Council and meet their standards to 'Maintain and protect patients' information.'

All dentists and registered members of the dental team, dental hygienists, therapists, dental nurses, orthodontic therapists, dental technicians must comply with the General Dental Council standards for Patient Confidentiality.

In England, the Health and Social Care Act 2008 has led to the formation of the Care Quality Commission (CQC), which sets out detailed requirements for records.[3]

Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (No 2936) states that:

- The registered person must ensure that service users are protected against the risks of unsafe or inappropriate care and treatment arising from a lack of proper information about them by means of the maintenance of:

- An accurate record in respect of each service user which shall include appropriate information and documents in relation to the care and treatment provided to each service user, and such other records as are appropriate.

The registered person must ensure that the records (which may be paper or electronic form) are:

- ✓ Kept securely and can be located promptly when required;
- ✓ retained for an appropriate period of time; and,
- ✓ securely destroyed when it is appropriate to do so.

Patients should be able to be confident that their personal records including medical records are accurate, fit for purpose, held securely, and remain confidential. Other records required to be kept, to protect their safety and well-being are maintained and held securely where required. [3]

Information Governance Compliance

In a UK dental practice, data protection responsibilities are shaped mainly by UK GDPR, the Data Protection Act 2018, and NHS guidance (if NHS services are provided). Not every role must be a separate person, but the functions must be covered.

Summary of roles and responsibilities

Role	Decision-Making Authority	Direct Responsibility for Compliance	Accountability	Required by Law?
Data Controller	Decides **why** and **how** data is processed.	Primary responsibility.	Accountable to supervisory authorities (e.g., ICO).	Always needed when processing personal data.

Data Processor	Acts under controller's instructions.	Directly accountable to ICO for processor duties.	Accountable to the controller and ICO.	Depends on whether the controller outsources processing.
Data Protection Officer	No decision-making power over processing.	Ensures compliance and provides advice.	Reports to the highest level of management.	Required in specific cases (e.g., public authorities, large-scale monitoring, special categories of data). Most dental practices are not legally required to appoint a DPO but may choose to do so.

Each dental practice needs to have a consistent approach to information handling and to do this it can be helpful for one or more members of staff to be assigned responsibility for organising and monitoring standards of information handling within the practice and for developing and implementing an Information Governance (IG) improvement plan. The Information Governance Lead should have sufficient seniority and authority to ensure that any necessary changes in information handling within the practice can be implemented and enforced, they may also carry out any of the above roles as well.[4]

What training does the Information Governance Lead need?

- ✓ UK GDPR and Data Protection Act 2018
- ✓ Confidentiality
- ✓ Information sharing and Freedom of Information Act requirements
- ✓ Ability to write policies, procedures and material for use by the team[4]

Training can be undertaken in-house or by a commercial training company or by accessing an e-learning course.

Responsibilities of an Information Governance lead[4]
• **Ensure there is an up-to-date IG policy in place**
• **Coordinate the management, assessment and reporting of any identifiable risks that take place**

• **Training for all members of staff and new members of staff and continually support them by implementing clear and robust data handling standards and procedures**
• **Monitor the information handling and sharing activities to ensure compliance with law and guidance within the practice**
• **Manage any requests for the sharing of information**
• **Ensure any required documentation is submitted to relevant organisations, e.g., General Dental Council, Care Quality Commission**
Ensuring patients are appropriately informed about the practice's information handling activities
• **Create an improvement plan and monitor and report when required**
• **Data breach management and incident reporting**
• **Records management and retention**
• **Cyber security basics (especially for DSP Toolkit)[4]**

Data Security Protection Toolkit

The DSP Toolkit is a required online checklist for any organisation that uses or accesses NHS health data. It helps dental practices show they follow UK data protection and cybersecurity rules, including the National Data Guardian's 10 Data Security Standards. It is a mandatory requirement for NHS dental practices and must be reviewed annually.

For private dental practices, completing the DSP Toolkit is important to stay compliant with NHS requirements and keep access to NHS services. The toolkit includes guidance, templates, and policies to help practices meet these standards.

Some private practices may find the process difficult, but support is available. For example, CODE provides an updated IG Improvement Plan (M217A) to help

complete the toolkit. Practices can also contact the NHS to get DSP Toolkit access and apply for an NHSmail account.

The updated DSP Toolkit now requires practices to publish a compliance statement, which is needed to meet the national data opt-out policy. Practices must also ensure that healthcare data is only used for direct patient care and treatment, as this is a key focus of the updated requirements.[4]

Information Governance Policy

The practice is required to have an Information Governance Policy which needs to be a statement of the intended approach to effectively implement Information Governance. The policy should outline the procedures in place that underpin the policy and set out what is expected of the dental team in order to ensure compliance.

As stated above, it is part of the role of the Information Governance Lead to develop and maintain the policy and this should be agreed with the senior management in the practice and the owner. Best practice requires that the policy is regularly reviewed and updated, and any necessary amendments are made.[5]

A template of a Policy can be accessed from the link at the end of the article to act as a guide. It can be tailored to suit your practice if you decide it is enough for your needs.

Information Governance Policy - Points to Consider[5]
A section specifying why the policy is required – i.e., to safeguard the movement of personal identifiable data in the practice
An overview of how information will be handled by the practice – maintenance of confidentiality, safe havens, storage of data, consent to view data, situations where disclosure may be required
A description of accountability and responsibility for the policy – i.e., details of who is the IG lead in the practice and job roles of any support staff

A process for monitoring the policy
Staff duties and responsibilities for information governance (maintaining confidentiality of data, ensuring secure storage of data, being aware of situations where disclosure may be required)
A description of how the various areas within the policy link together
Actions to be taken if the policy is breached – i.e., sanctions against staff, remedial work on the part of those responsible for IG procedure

Staff Training

It is essential that everyone working for or on behalf of the practice is fully informed about Information Governance (IG) procedures and given clear guidelines about their own individual responsibilities for maintenance of good IG practice.

Therefore, measures should be put in place to ensure that all staff members are fully informed of the procedures implemented to ensure Information Governance requirements are met.

The practice should ensure that appropriate IG training is made available to all staff, including temps, locums and volunteers. There should be a clearly documented and communicated process for making all staff aware of the availability and importance of training.[6]

- ✓ All staff should be provided with basic IG awareness training and informed where support and further information are available
- ✓ Emphasis should be placed on how the requirements affect their day-to-day work practices
- ✓ All staff members who have routine access to confidential information should be provided with additional IG training
- ✓ Ideally all new staff members should be provided with IG training within a short time of taking on their post
- ✓ Annual refresher training should be completed[6]

Gaining Consent

Practices need a lawful basis for processing personal and health data. In most clinical scenarios, the lawful basis is "necessary for provision of care." Patients must be informed of how their information is used and have access to their records under UK GDPR subject access provisions.

Dental practices do not usually rely on patient consent under UK GDPR as the legal reason for using personal data when providing dental care.

Instead, the law allows dental practices to use patient data because:

- It is necessary to provide healthcare, which is legally permitted under Article 9(2)(h) of UK GDPR (this covers medical diagnosis, treatment, and care).
- It is in the public interest to provide healthcare safely and effectively.

This does **not** remove the need for:

- Clinical consent to treatment
- Keeping patient data secure and confidential
- Using data only for appropriate healthcare purposes

The use of patient information and the procedures for sharing patient information is also governed by other legal provisions for example:

- The common law duty of confidence
- The Human Rights Act 1998
- NHS Act 2006
- The NHS Code of Practice on Confidentiality
- Professional Codes of Conduct and Standards
- The Caldicott Principles

Patients must be informed of their rights to access their own records and privacy policies should be clearly displayed in waiting areas.[7]

Although originally developed for NHS organisations, Caldicott Principles are widely adopted in healthcare information governance.

The Caldicott Principles – Published December 2020[9]
Principle 1: Justify the purpose(s) for using confidential information
Principle 2: Use confidential information only when it is necessary
Principle 3: Use the minimum necessary confidential information

Principle 4: Access to confidential information should be on a strict need-to-know basis
Principle 5: Everyone with access to confidential information should be aware of their responsibilities
Principle 6: Comply with the law
Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
Principle 8: Inform patients and service users about how their confidential information is used

Dental Record Retention

The retention period for dental records is not explicitly defined by UK GDPR or the Data Protection Act 2018. However, dental professionals are generally advised to retain records for a certain period after the last treatment. The retention period may vary depending on the type of record and individual circumstances.[10]

The NHS advice on retention in England and Wales recommends that records should be retained for 11 years and children's records should be retained until the 25th birthday or 26th birthday if the patient was 17 years when treatment was completed.[10]

The Scottish government provides guidance advising the recommended retention period for general dental records as 10 years for adults and 10 years or up to the 25th/26th birthday rule, whichever is longer for children.[10]

In Northern Ireland there is guidance on record retention from the Department of Health and contained within the Regulation and Improvement Authority (Independent Health Care) (Fees and Frequency of Inspections) (Amendment) Regulations (Northern Ireland) 2011.[10]

Securing the Premises and Equipment

It is important to ensure that the practice premises, equipment, records and staff are protected by physical security measures. Although this is routinely undertaken by practice managers, Information Governance requirements require procedures to safeguard the security of hardware, software and information.

Practices need to maintain accurate records of the type of storage they have for information, how many computers they use, how the information can be accessed on the premises or remotely. If remotely, how security is maintained. If memory sticks, smart phones or other PDAs or digital cameras are used, documentation needs to identify the user and how security is maintained.[10]

Consider the following:

1. The physical location of equipment; what software is used
2. Which internet provider is used; who is responsible for each computer
3. Who would be contacted if something went wrong
4. A written record of all of this information is essential for security[10]

Monitoring and Auditing

Regular monitoring and auditing of computing systems and remotely accessed devices should include, if possible, the point and location of use to ensure that unauthorised access is prevented and that all users comply with procedure and guidance. All mobile devices and removable media need to be accounted for, and sensitive or confidential information should be encrypted and securely transported and stored. Practices should ensure that any suppliers also adhere to this requirement.[11]

A risk assessment should be carried out to identify any areas of concern to ensure that there are procedures in place to detect any attempted unauthorised access to the premises or information. Staff training should outline any necessary procedures that they need to follow.[11]

Key Areas to Consider

- Window and door security
- Fire escapes
- Security of offices
- Security of paper records
- Computer workstation
- Monitor who holds keys to which areas

- Consider electronic keypads which can be changed as necessary
- Staff should be encouraged to clear desks of all sensitive and confidential information when it is no longer required for the task in hand
- Staff should also be informed of how to use a password protected screen saver on their computers if they need to leave their machine unattended[11]

Good Practice Guidance and Encryption

The dental team need to be informed of basic good practice steps to reduce the risk of theft and ensure patient confidentiality is maintained at all times. This should include:

- Locking machines up overnight or removing the hard-drive or memory card where possible
- Not leaving the system unattended e.g., laptops on seats in cars
- Using secure passwords to prevent unauthorised access the information stored on the computer
- Ensuring password security and regularly changing passwords
- Reporting lost or stolen equipment promptly[7]

Encryption

Wherever possible, information on laptops and PC hard drives should be encrypted. Full-disk encryption (BitLocker/File Vault) is recommended as best practice. If this is not possible, a risk assessment should be undertaken to ensure that data security is at an acceptable level to the practice to work to.

Only a minimum amount of data should be carried on mobile devices to reduce the potential impact of an unforeseen event causing loss of data.

All devices must have adequate virus protection and spyware that is regularly updated to prevent any types of attack.

The practice should ensure that only equipment belonging to the practice is used as allowing team members to use their own equipment could cause a potential data breach. [12]

Audits of Computer Systems

Regular audits should be undertaken to ensure the correct operational use of the system; to prevent unauthorised use; to ensure all users comply with the procedures and guidance set out by the practice; ensure all mobile devices and removable media devices can be accounted for; to ensure secure remote access is possible and is used and to ensure sensitive and confidential information is encrypted and securely transported if necessary.[13]

Incident management and reporting

All information governance incidents (loss, theft, breach, or near-miss) should be recorded and assessed. Practice policies should describe:

- How incidents are reported internally
- Risk assessment procedures
- Remedial actions taken
- When external reporting is required (e.g., to the Information Commissioner's Office if there is a risk to individuals' rights and freedoms, usually within 72 hours if feasible)
- Communication to affected patients where required[13]

Transfer of information

Possible modes of transfer of information include:

- Post/courier
- Personal Conversations
- Telephone
- Fax
- Email
- SMS Messaging
- Instant Messaging (IM)
- Web Interfaces
- Portable Data Storage Devices[14]

For the transfer of information in both hardcopy and digital formats there must be adequate protection from interception, copying, modification, misrouting and destruction. In the case of digital information (including email file attachments) this includes protection from malicious code. The practice will need to work with their IT system supplier to ensure that appropriate technical measures are in place, e.g., monitoring of communication traffic.[14]

If the post is being used to receive personal or sensitive information, it is essential that physical security measures are in place such as lockable doors/cabinets to protect information received by post.

Emails containing personal or sensitive information must be stored appropriately on receipt, e.g., incorporated within the individual's record, and deleted from the email system when no longer needed.[14]

Care should be taken when using WhatsApp in particular group messaging which many practices now use to ensure patient data is not used without the necessary security.

The practice should ensure the dental team are trained in the appropriate method of transfer of information e.g., post, email, fax. How much information can be given on the phone, how to record information e.g., message book, discussions with patients in public areas, where records are stored and how long information should be retained for.[14]

Conclusion

Information governance is a legal and ethical obligation for UK dental practices. By maintaining robust policies, appropriate training, secure systems, and effective incident management, teams can fulfil regulatory standards, protect patient confidentiality and deliver safe, trustworthy care.

Personal Development Plan and Reflective Learning

This CPD is linked to the following GDC Enhanced CPD Development Outcomes:

B. Effective management of self, and effective management of others or effective work with others in the dental team, in the interests of patients at all times; providing constructive leadership where appropriate.

C. Maintenance and development of knowledge and skill within your field of practice.

D. Maintenance of skills, behaviours and attitudes which maintain patient confidence in you and the dental profession and put patients' interests first.

Reflective learning is now a requirement of the GDC Enhanced Professional Development Scheme. As such, you will now have the opportunity to answer some reflective learning questions, if you complete these now you will fulfil the requirements of the GDC. These will be:

1) What did you learn (or confirm) from the activity that was helpful or relevant to your daily work and patients?
2) Comment on any changes/updates needed in your daily work
3) How has completion of this CPD article benefitted your work as a DCP?

Further Reading

Example of An Information Governance Policy

https://www.england.nhs.uk/ig/about/

Health information | ICO

References:
1. DDU (2026) https://www.theddu.com/guidance-and-advice/guides/protecting-patient-data (accessed 01/01/2026).
2. General Dental Council (2020) https://standards.gdc-uk.org/pages/principle4/principle4.aspx (accessed 01/01/2025).
3. CQC (2022) Available from https://www.cqc.org.uk/guidance-providers/all-services/check-way-you-handle-personal-information-meets-right-standards (accessed 01/01/2026).
4. NHS (2025) Available from: https://www.dsptoolkit.nhs.uk/ (accessed 01/01/2026).
5. CQC (2020) https://www.cqc.org.uk/sites/default/files/20190228%20CQC%20Information%20Governance%20Policies.pdf (accessed 01/01/2026).
6. DDU (2022) https://www.theddu.com/guidance-and-advice/guides/information-governance-in-dental-practices (accessed 01/01/2026).
7.NHS (2023) https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/#introduction (accessed 01/01/2026).
8 DDU (2025) Available from: https://www.theddu.com/guidance-and-advice/guides/retaining-and-destroying-patient-records (accessed 01/01/2026).

9 National Data Guardian (2020) available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf (accessed 01/01/2026).
10 NHS England (2023) Available from: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/ (accessed 01/01/2026).
11. ICO (2025) https://ico.org.uk/for-organisations/the-guide-to-nis/security-requirements/ (accessed 01/01/2026).
12. ICO (2025) https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/data-storage-sharing-and-security/ (accessed 01/01/2026).
13. CQC (2020) https://www.cqc.org.uk/guidance-providers/all-services/check-way-you-handle-personal-information-meets-right-standards-0 (accessed 01/01/2026).
14 ICO (2022) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/ (accessed 01/01/2026).