Professional Certificate in Dental Compliance

Data Protection and Information Governance

Data Protection and Information Governance Glossary

1. Data Protection
Data protection refers to the process of safeguarding personal data from unauthorized access, use, disclosure, disruption, modification, or destruction. This is crucial in ensuring that individuals have control over their personal information and that it is processed fairly and lawfully. In the context of the Professional Certificate in Dental Compliance, data protection is essential for complying with regulations such as the General Data Protection Regulation (GDPR) to protect patient information.

2. Information Governance
Information governance involves the management of information in a way that promotes accountability, transparency, and compliance with relevant laws and regulations. It encompasses the policies, procedures, and controls that ensure information is handled securely and in accordance with legal requirements. In the dental industry, information governance is vital for maintaining the confidentiality and integrity of patient records.

3. GDPR (General Data Protection Regulation)
The GDPR is a comprehensive data protection regulation that came into effect in the European Union in 2018. It imposes strict requirements on organizations that collect, process, and store personal data, including dental practices. Compliance with the GDPR involves implementing measures to protect patient information, obtaining consent for data processing, and ensuring the rights of individuals are respected.

4. Personal Data
Personal data refers to any information that relates to an identified or identifiable individual. This can include names, addresses, phone numbers, email addresses, medical records, and other details that can be used to identify a person. Dental practices collect and process personal data as part of providing healthcare services, making it essential to protect this information from misuse or unauthorized access.

5. Consent
Consent is a fundamental principle of data protection that requires individuals to give their explicit permission for their personal data to be collected, processed, or shared. In the context of dental compliance, obtaining valid consent from patients before accessing their medical records or sharing their information with third parties is crucial to ensure compliance with data protection regulations.

6. Data Controller
A data controller is an individual or organization that determines the purposes and means of processing personal data. In the context of a dental practice, the practice owner or manager is typically the data controller responsible for ensuring that patient information is handled in compliance with data protection laws and regulations.

7. Data Processor
A data processor is a person or entity that processes personal data on behalf of the data controller. This can include third-party service providers or software vendors that handle patient information as part of providing services to a dental practice. Data processors are required to comply with data protection regulations and maintain the security of the data they process.

8. Data Breach
A data breach occurs when there is unauthorized access to or disclosure of personal data. This can happen due to cyberattacks, human error, or system vulnerabilities, putting individuals' information at risk of misuse or theft. Dental practices must have procedures in place to detect, report, and mitigate data breaches to protect patient confidentiality and comply with data protection requirements.

9. Information Security
Information security involves the measures and controls implemented to protect the confidentiality, integrity, and availability of information. This includes safeguarding data from unauthorized access, ensuring data accuracy and consistency, and maintaining data availability for authorized users. In the context of dental compliance, information security is essential for protecting patient records and preventing data breaches.

10. Privacy Impact Assessment (PIA)
A Privacy Impact Assessment is a systematic process for assessing the privacy risks associated with the collection, use, and disclosure of personal data. Conducting a PIA helps organizations identify potential privacy issues, evaluate the impact of data processing activities on individuals' privacy rights, and implement measures to mitigate risks. Dental practices can use PIAs to assess the privacy implications of new processes or technologies that involve patient data.

11. Data Subject
A data subject is an individual who is the subject of personal data. In the context of a dental practice, patients are considered data subjects whose personal information is collected, processed, and stored for the purpose of providing healthcare services. Data subjects have rights under data protection laws, including the right to access their data, request corrections, and withdraw consent for data processing.

12. Data Retention
Data retention refers to the practice of storing personal data for a specified period of time before securely disposing of it. Dental practices must establish data retention policies that define how long patient records should be kept, taking into account legal requirements, patient consent, and the need to maintain accurate and up-to-date information. Proper data retention practices are essential for information governance and compliance with data protection regulations.

13. Encryption
Encryption is the process of converting data into a secure format that can only be accessed by authorized users with the appropriate decryption key. This helps protect sensitive information from unauthorized access or interception during transmission or storage. Dental practices can use encryption technologies to secure patient records, communications, and other data to prevent data breaches and safeguard patient

confidentiality.

14. Access Controls
Access controls are security measures that restrict access to data, systems, or facilities to authorized users only. This helps prevent unauthorized access, data breaches, and misuse of information by ensuring that individuals can only access the data they are authorized to view or modify. In the context of dental compliance, access controls are essential for protecting patient records and maintaining data security.

15. Data Minimization
Data minimization is the principle of collecting and retaining only the personal data that is necessary for a specific purpose. By minimizing the amount of data collected and processed, organizations can reduce privacy risks, enhance data security, and comply with data protection regulations. Dental practices should adopt data minimization practices when collecting patient information to limit the exposure of sensitive data and protect patient privacy.

16. Information Governance Framework
An information governance framework is a structured approach to managing information assets, policies, procedures, and controls within an organization. It provides a framework for ensuring that information is handled securely, efficiently, and in compliance with legal requirements. In the context of dental compliance, an information governance framework helps dental practices establish best practices for managing patient records, data protection, and compliance with regulatory requirements.

17. Record Keeping
Record keeping involves the creation, maintenance, and retention of accurate and complete records of patient information, treatments, and interactions. Proper record keeping is essential for delivering quality healthcare, ensuring patient safety, and complying with legal and regulatory requirements. Dental practices must establish record keeping policies and procedures to maintain accurate patient records, protect confidentiality, and facilitate continuity of care.

18. Electronic Health Records (EHR)
Electronic Health Records (EHR) are digital versions of patients' paper charts that contain medical history, diagnoses, treatment plans, medications, and other healthcare information. EHR systems enable dental practices to store, access, and share patient records electronically, improving efficiency, accuracy, and accessibility of information. Protecting EHR data from unauthorized access, data breaches, and cyber threats is essential for maintaining patient confidentiality and complying with data protection regulations.

19. Data Privacy Officer (DPO)
A Data Privacy Officer (DPO) is a designated individual within an organization responsible for overseeing data protection and privacy compliance. The DPO ensures that the organization processes personal data in accordance with data protection laws, responds to data subject requests, and monitors compliance with data protection regulations. In the context of a dental practice, appointing a DPO is essential for managing data protection policies, procedures, and practices to protect patient information and comply with legal requirements.

20. Data Mapping

Data mapping is the process of identifying, classifying, and documenting the flow of personal data within an organization. This helps organizations understand where data is collected, processed, stored, and shared, enabling them to assess privacy risks, implement data protection measures, and comply with regulatory requirements. Dental practices can use data mapping to identify the types of patient information they collect, how it is used, and who has access to it to ensure compliance with data protection regulations.

21. Breach Notification
Breach notification is the process of informing relevant authorities and individuals about a data breach that may compromise the security of personal data. Under data protection regulations such as the GDPR, organizations are required to report data breaches to the appropriate supervisory authority and notify affected individuals without undue delay. Dental practices must have breach notification procedures in place to respond promptly to data breaches, protect patient information, and comply with data protection requirements.

22. Data Subject Rights
Data subject rights are the rights that individuals have over their personal data under data protection laws. These rights include the right to access their data, request corrections, object to data processing, withdraw consent, and request erasure of their information. Dental practices must respect and uphold data subject rights to protect patient privacy, ensure transparency, and comply with data protection regulations.

23. Secure Disposal
Secure disposal involves the proper destruction of personal data that is no longer needed or required to be retained. This includes shredding paper records, deleting electronic files, and securely disposing of physical media to prevent unauthorized access, data breaches, and identity theft. Dental practices must have secure disposal procedures in place to protect patient information, maintain data security, and comply with data protection requirements.

24. Data Security Policy
A data security policy is a set of guidelines, procedures, and controls that outline how personal data should be handled, protected, and secured within an organization. Data security policies define roles and responsibilities, specify data protection measures, and establish safeguards to prevent unauthorized access, data breaches, and misuse of information. Dental practices should develop and implement data security policies to protect patient records, maintain data integrity, and comply with data protection regulations.

25. Privacy by Design
Privacy by Design is a concept that promotes building privacy and data protection measures into the design and development of systems, products, and processes from the outset. By embedding privacy principles into the design of information systems, organizations can enhance data security, protect individual privacy, and comply with data protection regulations. In the context of dental compliance, adopting Privacy by Design principles helps dental practices minimize privacy risks, ensure data protection, and build trust with patients.

26. Data Audit
A data audit is a systematic review and assessment of an organization's data processing activities, data

flows, and data protection practices. Data audits help organizations identify privacy risks, assess compliance with data protection regulations, and implement measures to protect personal data. Dental practices can conduct data audits to evaluate how patient information is collected, used, and stored, identify vulnerabilities, and strengthen data protection measures to comply with regulatory requirements.

27. Data Integrity
Data integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. Maintaining data integrity ensures that information is complete, trustworthy, and free from errors or unauthorized modifications. Dental practices must implement controls and safeguards to protect data integrity, prevent data loss or corruption, and maintain the quality and reliability of patient records to ensure compliance with data protection regulations.

28. Information Sharing
Information sharing involves the exchange of personal data between healthcare providers, organizations, or individuals for the purpose of delivering healthcare services, coordinating care, or fulfilling legal requirements. Sharing patient information is essential for providing quality healthcare, ensuring continuity of care, and complying with regulatory obligations. Dental practices must establish policies and procedures for secure information sharing to protect patient confidentiality, maintain data security, and comply with data protection regulations.

29. Data Transfer
Data transfer refers to the movement of personal data from one location to another, such as between healthcare providers, systems, or jurisdictions. When transferring patient information, organizations must ensure that data is protected, secure, and compliant with data protection regulations to prevent unauthorized access, data breaches, or privacy violations. Dental practices must implement safeguards and controls to secure data transfers, maintain data integrity, and protect patient confidentiality in compliance with regulatory requirements.

30. Data Governance
Data governance is a framework of policies, procedures, and controls that ensures data is managed effectively, securely, and in compliance with legal requirements. Data governance encompasses data quality, data security, data privacy, and data management practices to protect information assets, maintain data integrity, and support organizational objectives. In the context of dental compliance, data governance is essential for managing patient records, protecting confidentiality, and complying with data protection regulations.