**Dental record management**

Page 2 of 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **1** | **There is a system in place for managing dental records safely and securely** |
|  | Processes are in place to ensure that the management of patient records complies with the principles of the Data Protection Act, including secure storage (paper and electronic records), maintenance of patient data and subject access requests. |[ ] [ ]        |
|  | Processes are in place to ensure that documents which are not part of the dental record are stored appropriately.*(e.g. complaints)* |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **2** | **There is a system for creating new patient records**  |
|  | The patient’s personal details and contacts have been checked for accuracy. |[ ] [ ]        |
|  | The patient has had a medical history form completed before commencing treatment. |[ ] [ ]   |
|  | All relevant forms e.g. GP17, FP17, FPW17 have been commenced. |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **3** | **There is a standardised system for processing records when a patient leaves the practice** |
|  | The record is archived as appropriate and retained for 11 years, or in the case of children until they reach 25 years of age, whichever is the longer. |[ ] [ ]        |
|  | Retention includes all clinical records, radiographs, study models and photographs etc. |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **4** | **The patient system provides a secure and accessible audit trail** |
|  | All employed staff with access to the patient system have individual logins and secure passwords. |[ ] [ ]        |
|  | Users log out of computers when unattended. |[ ] [ ]   |
|  | All attached healthcare professionals with access to the patient system have their own logins and secure passwords. |[ ] [ ]   |
|  | It is always clear who has accessed patient records and carried out specific tasks and actions. |[ ] [ ]   |
|  | The audit trail for electronic records is available for checking and training purposes. |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **5** | **There is a clear system for dealing with discovered misfiling**  |
|  | Individual and team responsibilities are clear. |[ ] [ ]        |
|  | If information is incorrectly recorded in another patient’s record, an entry is made in both sets of notes when this is resolved to ensure transparency. |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **6** | **There are robust policies for business continuity and data recovery** |
|  | There is a comprehensive Business Continuity Plan in place. |[ ] [ ]        |
|  | Procedures are clear in the event of a breach of security and/or data loss. |[ ] [ ]   |
|  | Secure back-up arrangements include individual responsibilities, documentation, back-up verification and arrangements for deputising responsibilities.  |[ ] [ ]   |
|  | IT support is readily available. |[ ] [ ]   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **7** | **There is a secure system for disposal of confidential waste/scanned documents** |
|  | External suppliers are checked for system compliance with Data Protection standards. |[ ] [ ]        |
|  | Assurance is obtained that all employed staff within external suppliers are aware of responsibilities in relation to confidentiality. |[ ] [ ]   |