

**HIPAA-3**

This document is a **HIPAA checklist** for dental clinics, covering important topics such as patient information protection, privacy rules, risk analysis, and breach reporting.

* The checklist covers various HIPAA items that dental clinics need to comply with.
* It emphasizes the importance of protecting patient's health, financial, and personal information.
* The checklist mentions the need to know the privacy rule, security rule, HITECH act, and patient's rights.
* It also highlights the requirement for Texas clinics to conform with Texas House Bill-300 (HB-300).
* The checklist mentions errors that dental clinics have made during the transfer of physical information to a digital format.
* It explains the role of the Privacy Rule in protecting the digital flow of patient's PHI.
* The checklist lists the different identifiers that can be considered as patient's personal information.
* It clarifies the distinction between Covered Entities and Business Associates in terms of HIPAA consent.
* The checklist mentions the importance of limiting disclosure of patient information and providing access to patients.
* It emphasizes the penalties and enforcement measures for HIPAA violations.
* **You must use this form annually to check the compliance of the clinic as it paves a pathway towards COMPLIANCE in HIPAA**

******

Clinic Name: Date:

HIPAA Checklist

**Choose**

**Select/click the appropriate box. Only choose the column Y (yes) if you can provide proof during an audit.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |
| **#** | **HIPAA Item (Based on Safety Needs)** | **Y** | **N** | **N/A** | |
| 1 | It is called HIPAA and not Hippa. |  |  |  | |
| 2 | Health information Portability and Accountability Act (HIPAA) protects patient’s and helps  reduce misuse of the information, |  |  |  | |
| 3 | Every dental clinic must protect the patient’s health, financial and personal information. |  |  |  | |
| 4 | Your clinic must protect patient information, know the privacy rule, security rule, the HITECH act  and the patient’s rights. |  |  |  | |
| 5 | Clinics in Texas must also conform with the Texas House Bill-300 (HB-300). |  |  |  | |
| 6 | Dental clinics committed errors during transfer of physical information to a digital format. |  |  |  | |
| 7 | The Privacy Rule protects the digital flow or use of the patient’s PHI. |  |  |  | |
| 8 | Patient’s Personal Information could contain one of the following identifiers—Name, ZIP Code,  Address, Telephone Number, Date of Birth and Social Security Number. |  |  |  | |
| 9 | You can freely share de-identified patient information. |  |  |  | |
| 10 | Dentists, Dental Labs, Referral Specialty Dental Clinics, Pharmacies, Medical Labs used by the dentist Dental Insurance plans, and healthcare billing/clearing house are Covered Entities and do not need further HIPAA consent by the patient to share patient information.  Agencies, CPAs and lawyers hired by the clinic are Business Associates. |  |  |  | |
| 11 | An associate dentist has full access to all the patients of the clinic automatically. |  |  |  | |
| 12 | Other than sharing with Covered Entities for patient care, you must limit disclosure of patient  information. |  |  |  | |
| 13 | Patients normally have access to their information even if it is in the dental chart. |  |  |  | |
| 14 | Clinics can charge a nominal charge to give a patient usable information. |  |  |  | |
| 15 | State Law will not prevail if federal law id stronger. |  |  |  | |
| 16 | HIPAA enforcement penalties may be as much as 1.5 million dollars and imprisonment. |  |  |  | |
| 17 | An encrypted sharing method between entities is needed for safe sharing of patent  information. |  |  |  | |
| 18 | You cannot go back and alter or destroy patient information without the ‘time and date’  of the alteration/destruction being recorded by the EHR. |  |  |  | |
| 19 | Confidentiality, Integrity, and Availability of the patient information is vulnerability. |  |  |  | |
| 20 | Every clinic must conduct Risk Analysis and implement Risk Management measures. |  |  |  | |
| 21 | It is easier to let a firm, or even a trained person handle your clinic’s end-point-  security. |  |  |  | |
| 22 | Access to information, workforce security for employees, and BA contracts for BAs are  needed to make sure patient information is protected. |  |  |  | |
| 23 | Administrative safeguards and technical safeguards are two main components of Risk  Analysis and Risk Management. |  |  |  | |
| 24 | By controlling the access of your employees to your network/computers with a  password, you can implement a technical safeguard in protecting patient information. |  |  |  | |
| 25 | Threats to your systems can be Natural, Human or Environmental. |  |  |  | |
| 26 | An ex-employee’s must not be able to access the system which contains patient  information. |  |  |  | |
| 27 | A threat can be either of a high-likelihood, a medium-likelihood, or a low-likelihood. |  |  |  | |
| 28 | You should first concentrate reducing the high and medium likelihoods of a threat. |  |  |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 29 | It is very important for the clinic owner to be involved in Risk Analysis and Risk  Management. |  |  |  |
| 30 | The clinic must do a periodic review (at least annually) and document the audit. |  |  |  |
| 31 | If you know of a data breach your clinic is engaged in, you must inform patients of the  breach satisfying HIPAA rules based on the size of the breach. |  |  |  |
| 32 | If the breach involves more than 500 patients, it is considered a large breach. |  |  |  |
| 33 | The HHS has a form to report breaches. |  |  |  |
| 34 | HITACH Act expands on the privacy rule and gives patients more rights. |  |  |  |
| 35 | Federal HIPAA states that you must provide the patient information within 30 days. |  |  |  |
| 36 | It is always presumed a breach unless you can demonstrate a low probability. |  |  |  |
| 37 | Federal HIPAA says that all employees must be trained within 90 days of employment. |  |  |  |
| 38 | You should avoid discussing PHI other than for patient care activities. |  |  |  |
| 39 | You can destroy temporary patient information to protect PHI. |  |  |  |
| 40 | You must return patient information to its place of storage at the end of the day. |  |  |  |
| 41 | You can use a computer screen privacy filter to protect patient information. |  |  |  |
| 42 | In a school or a hospital (large entity), you should wear an ID badge for security. |  |  |  |
| 43 | You must not use unencrypted platforms or emails in sharing PHI. |  |  |  |
| 44 | You must not use unencrypted mobile device in using or collecting PHI. |  |  |  |
| 45 | You must not leave PHI unmonitored on the printer or fax machine. |  |  |  |
| 46 | You must use internet and digital security measures (such and not succumbing to  Phishing, Whaling, and attacks by Bots) |  |  |  |
| 47 | You should update software and upgrade hardware as needed. |  |  |  |
| 48 | You should lock and Key approach for physical data storage and cash. |  |  |  |
| 49 | Your clinic should not allow sharing of passwords and should make users change passwords periodically. |  |  |  |
| 50 | You should keep the voice low while speaking to a patient. |  |  |  |
| 52 | You should provide privacy such as closing the door or provide privacy. |  |  |  |
| 52 | You should flip over patient charts and other printed patient information so that  unauthorized people don’t have access, |  |  |  |
| 53 | You must not take PHI outside the clinic using flash drives, smartphones and laptops. |  |  |  |
| 54 | You must not access PHIs using unprotected Wi-Fi. |  |  |  |
| 55 | Your clinic must have a policy on temporary information, cheques, credit cards and  cash handling. |  |  |  |
| 56 | You must not use the patient’s information for other than treatment without additional  signed consent of the patient or guardian (such as for marketing use) |  |  |  |
| 57 | You must get the patient’s signed HIPAA authorization for treatment before providing  treatment. |  |  |  |

Audit Conducted by:

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: Designation:

******