（第１号様式）

資料２

安全管理措置報告書（記載例）

|  |  |  |  |
| --- | --- | --- | --- |
| 調査項目 | | 内容 | |
| １ 業者名  （医療機関名） | | 〇〇呼吸器内科クリニック  チェックは不要です  □横浜市競争入札有資格者　□その他（　　　　　　　　　　　　　）  □横浜市出資法人（条例第　条） | |
| ２ 業務の作業担当部署名 | | 医事課、もしくは上記１同様の医療機関名 | |
| ３ 業務の現場責任者役職名 | | 院長  本件業務における個人情報の取扱者の総数を記載  正社員に限らず派遣社員、アルバイト等の人数も含む | |
| ４ 業務の個人情報取扱者の人数 | | 10人 | |
| ５ 個人情報保護関連資格等 | | ■Ｐマーク　■ＩＳＭＳ  第三者機関が認定している資格等がある場合にチェック  該当なければ記載なし  □その他の資格（　　　　　　　　　　　　　　　　　　　　　　）  ■個人情報関係の損害保険に加入 | |
| ６ 個人情報保護に関する社内規程等 | | ■個人情報の使用、保存、廃棄等に関する管理規程  ■個人情報漏えい･紛失･滅失･盗難等事故時の対応規程・マニュアル等  ■個人情報保護について従業員との雇用契約や誓約書等に明記  ■その他の規程（個人情報保護方針を別途定めている。　　　　　）  □規程なし | |
| ７ 個人情報保護に関する研修・教育 | | ■個人情報保護に関する研修・教育を実施（年１回／従業員１人につき）  ■その他（新たに雇用した者に対しては雇用時に研修を実施　） | |
| ８ 個人情報保護に関する点検・検査・監査の方法等 | | 情報セキュリティ外部監査（年１回）  院内で定期的に点検実施 | |
| ９ 漏えい等の事案の対応規程・マニュアル等の内容 | | | |
|  | (1) 対応規程・マニュアル等がある場合 | 名　称 | 事故対応マニュアル |
| 内　容 |  |
| ・第１章　漏えい等事故・・・事故の定義について規定  ・第２章　事故の対応　・・・事故発生時の対応フローについて規定  ・第３章　事故の報告　・・・事故報告のタイミング、報告先について規定  ・第４章　その他　　　・・・社内罰則等について規定  マニュアルの目次等とともにその内容について、記載 | |
| (2) 対応規程・マニュアル等がない場合 | （漏えい等の事案が発生した場合にどのような対応を取るのかについて、なるべく具体的に記載していください。）  委託等先が個人事業主等で漏えい事故マニュアル等を作成・保有していない場合には、当該欄に、事故発生時の初期対応、事故に係る報告に関する事項等について、具体規定に記載 | |
| 10 個人情報を取り扱う作業場所の管理体制  院内のみでの作業かつ、電子カルテ使用の場合には  （２）、（４）、（５）を記入してください  ※ 作業を実施機関の施設内部のみで行い、かつ、受託者が、実施機関所有のＰＣ、タブレット等の電子計算機のみを使用する場合には記入不要です。作業を実施機関の施設内部のみで行い、かつ、受託者所有の電子計算機を使用する場合には、(2)電磁媒体の項目、(4)及び(5)を記入してください。 | | | |
|  | (1) 作業施設の入退室管理 | 作業期間中の入室可能人数  □上記４の作業者のみ  ■作業者以外の入室可（■上記外80名　□その他）  入退室者名及び時刻の記録  □なし　（施錠のみ、身分証提示のみ等）  ■あり　■用紙記入  ■ＩＣカード等によりＩＤ等をシステムに記録  ■カメラや生体認証等により特定個人の入退室時刻を記録  □その他（　　　　　　　　　　　　　　）  　□その他（　　　　　　　　　　　　　　　　　　） | |
|  | (2) 個人情報の保管場所 | 紙媒体 | ■鍵付き書庫　■耐火金庫　■専用の保管室  取扱いがない場合は、その他欄に「取扱いなし」と記載 |
| □その他（　　　　　　　　　　　　　　　　　　　） | |
|  | 電磁媒体 | □鍵付き書庫　□耐火金庫　□専用の保管室 |
| ■その他（　使用場所にて保管　　　　　　　　　　　　　　　　　　） | |
|  | (3) 作業施設の防災体制 | □常時監視　■巡回監視　■耐火構造　■免震・制震構造  電子カルテの場合で特に使用場所より移動がない場合はその他に記載  □その他（　　　　　　　　　　　　　　　　　　　） | |
|  | (4) 個人情報の運搬方法 | 紙媒体 |  |
|  | 運搬を行わない場合や禁止する場合は、その旨を記載 | |
|  | 電磁媒体 |  |
|  | 運搬なし  運搬を行わない場合や禁止する場合は、その旨を記載 | |
|  | (5) 個人情報の廃棄方法 | 紙媒体 |  |
|  | 不要となった時点及び契約終了時に速やかに裁断処理します。 | |
|  | 電磁媒体 |  |
|  | 不要となった時点及び契約終了時に、速やかに、復元不可能な方法により削除し、CD-R等の外部記録媒体は物理的破壊を行った上で廃棄します。 | |
|  | (6) 施設外で作業を行う場合の個人情報保護対策（行う場合のみ記入） |  | |
| 11 電算処理における個人情報保護対策  ※紙媒体しか取り扱わない業務を行う場合は記入不要です。 | | | |
|  | (1) 作業を行う機器 | ■限定している（ノート型３台、デスクトップ型０台）  □限定していない | |
|  | (2) 外部との接続 | □作業機器は外部との接続をしていない  ■作業機器は外部と接続している  接続方法：□インターネット　■専用回線　□その他（　　　　　　　）  通信の暗号化：■している　□していない | |
|  | (3) アクセス制限 | ■ＩＤ・パスワード付与によりアクセス制限をしている  ＩＤの設定方法（個人情報を取り扱う従業者ごとにＩＤを付与）  パスワードの付け方（セキュリティレベルが高いパスワードを設定する。）  □ＩＤ・パスワード付与によりアクセス制限をしていない | |
|  | (4) 不正アクセスを検知するシステムの有無 | ■あり（検知システムの概要：ＩＰＳシステム　　　　　　　　　）  □なし | |
|  | (5) マルウェアを検知するシステムの有無 | ■あり（検知システムの概要：ＩＰＳシステム　　　　　　　　　）  □なし | |
|  | (6) ソフトウェアの更新 | ■常に最新のものに自動アップデートするものとなっている  □上記以外（　　　　　　　　　　　　　　　　　　　　　　　　　　　） | |
|  | (7) アクセスログ | ■アクセスログをとっている（３年保存）  □アクセスログをとっていない | |
|  | (8) 停電時のデータ消去防止対策 | ■無停電電源装置　■電源の二重化  □その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　）  □なし | |
|  | (9) その他の対策 |  | |
| 12 外国における個人情報の取扱いの有無 | | □あり  　□外国のサーバ上に個人情報が保存されているが、外国のサーバ上での個人情報の取扱いはない  　□外国のサーバ上に個人情報が保存されており、外国のサーバ上で個人情報を取り扱っている  ■なし  ※「あり」の場合は、以下も記入してください。 | |
|  | (1) 個人情報の取扱いがある外国の名称 |  | |
|  | (2) 当該外国における個人情報の制度・保護措置等 |  | |

ＩＤ・パスワードの設定方法について具体的に記載

なお、パスワードの定義（桁数等）は記載しないこと