

【個人情報管理体制】	
☐	経営層が、個人情報の適正な取り扱いに積極的に取り組む姿勢を法人や利用者に示している
☐	経営層が、管理者層が個人情報保護法や厚生労働省ガイドラインの基本的知識を有している
☐	個人情報保護に関する「基本方針」を策定し、公表している
☐	個人情報保護に関する「利用目的」を策定し、公表している
☐	全ての職員に基本規定が周知徹底されている
☐	個人情報保護に関する統括責任者が明確になっている
☐	個人上の適正な取扱いの組織図を策定している
☐	ほかの事業分野よりも一層適正な取扱いが求められていることを、従業員全員に周知徹底するための「仕組み」がある
☐	厚生労働省ガイドラインの内容を従業員全員に周知徹底させている
☐	個人情報保護に取り組む委員会がある
【個人情報の利用目的の明示と取得】	
☐	取得に際し、個人情報がどの様に利用されるのかを利用者が容易に理解できるように利用目的が特定されている
☐	利用目的が書面や院内・事業所内掲示、ホームページなど利用者に向けて公表されている
☐	本人から直接個人情報を取得する場合、書面にて利用目的を明示し、本人の同意を書面にて得ている
☐	患者・利用者から同意を得るに際し本人の判断能力に応じた丁寧でわかりやすい説明や対応を行っている
☐	患者・利用者向けに個人情報保護に関する事項について説明した書面を用意している
☐	個人情報データを正確かつ最新の内容に関する事項について説明した書面を用意している
☐	個人情報の取得で利用目的の範囲を超える場合には、本人の同意を得ることとなっている
【安全管理措置】 ①組織的安全管理	
☐	事業所に個人情報保護に必要な基本規定を整備し、従業員に周知している
☐	アクセス権限など情報システムの安全管理に関する規定を整備している

☐	書面、電磁媒体を含めた文書管理規定を整備し、従業員に通知している
☐	文書管理簿など、個人情報保護に関する帳簿類を整理している
☐	諸規定を、定期的または必要に応じて見直す体制となっている
☐	厚生労働省ガイドラインを必要な部署に常備している
☐	個人情報の相談苦情窓口担当者には、個人情報保護に関する十分な知識を有する者を選任している
☐	個人情報の統括責任者による管理・監査が適正に行われている
☐	個人データの安全管理のために、定期的な内部監査や自己評価を行い、改善を図っている
☐	漏えい等の問題が発生した場合の報告連絡体制が整備されている
☐	個人データ漏えい等の問題が発生した場合の「対応手順書」が整備されている
☐	複数の施設・事業所毎の安全管理措置が講じられ連携が取れた状態となっている
☐	雇用契約書や就業規則、誓約書に、就業期間中はもとより退職後も含めた守秘義務、個人情報保護が定められている

②人的管理

☐	個人情報保護に関し、正規職員だけでなく、パート職員、ボランティア、実習生に対しても誓約書を取り付けている
☐	就業規則に守秘義務違反、個人情報保護違反による罰則、懲戒規定が定められている
☐	個人情報の適正な取扱いに関し、従業員に対する教育・研修を実施している
☐	パート職員、ボランティア、実習生に対して、個人情報の適正な取扱いに関する教育・研修や監督を実施している
☐	従業員の採用時に、個人情報保護に関する教育・研修を実施している
☐	従業員への教育・研修を、定期的にまたは必要に応じて見直す体制となっている
☐	個人情報を取り扱うパソコンでの私的なインターネット使用、電子メールの使用は原則禁止とし、周知徹底している

③物理的安全管理

☐	個人データの重要度により院内、事業所内の区域管理を行っている
☐	個人データのアクセス管理や盗難、紛失を防止するため、入退館・入退室の管理を実施している

☐	正規職員、パート職員、ボランティアに対して従業員である身分を証明するものの着用を義務付けている
☐	記録、書類などをキャビネットや収納ケースの施錠管理を実施している
☐	個人データを情報機器で取り扱っている場合、コンピューター情報システムの運用管理に関する「手順書」を整備し、従業員に周知徹底している
☐	個人データを取り扱う情報機器に対する物理的な保護対策を講じている

④技術的安全管理

☐	個人データを取り扱うコンピューター等について、IDやパスワードによる認証などのアクセス管理を実施している
☐	個人データに関し、アクセスできる担当者を限定している
☐	個人データに関し、必要範囲にのみアクセス可能なルールとしている
☐	個人データにアクセスした従業員が特定できるようにIDとパスワードなどを採用し、その記録が保存されるシステムになっている
☐	個人データに対するファイアウォールを設置している
☐	個人データを管理するパソコンとインターネットに常時接続しているパソコンとは業務を区別して使用している
☐	情報機器に対して定期的にウィルスチェックを行っている
☐	情報機器の操作マニュアルを騎乗などに放置することを禁止している
☐	個人データの管理区域外の持ち出しを規制、管理している
☐	個人所有のノートパソコンを持ち込む際は文書管理責任者に許可を得て行い、その記録をつけている
☐	個人情報保管された外部記録媒体や事業所のノートパソコンなどを持ち出す場合には、文書管理者に許可を得て行い、その記録を付ける
☐	個人データの出力・コピー・ダウンロードをする場合は、文書管理責任者に許可を得て行い、その記録をつけている
☐	印字された個人情報は施錠されたキャビネットや部屋に保管している
☐	メール使用に関するマニュアルを作成し、従業員に周知徹底している

【廃棄】

☐	保管している個人データを廃棄する場合、その廃棄基準と廃棄手続きを明確なマニュアルとして定めている
☐	個人データの媒体ごとに保存期間を定めている
☐	個人データの媒体の保存期間満了後、当該帳票を廃棄する際に文書管理記録帳に記録をのこしている
☐	不要となった個人データの媒体の廃棄方法として、物理的な破壊、溶解、焼却など、復元・再生不可能になる方法を取っている

☐	個人データを取り扱った情報機器を廃棄する場合、記録装置内の個人データが復元・再生不可能になる方法をとっている
☐	患者・利用者の死亡後においても、その個人情報と同等の安全管理を講じている
☐	個人情報の漏えい等の事態が生じた場合の事業者の損害を補てんする損害保険に加入している

【業務委託】

☐	個人情報を取り扱う業務を外部業者に委託する場合、選定基準を設け、個人情報を適切に取り扱っている事業者を選定している
☐	個人情報を取り扱う業務を委託するに際し、委託契約書を交わしている
☐	委託元における安全管理と同内容の対策を講じるべきことを委託先の義務として規定している
☐	契約期間中・委託終了後における個人情報保護・守秘義務が規定されている
☐	委託先の業務が適切に行われていることを定期的を確認している
☐	委託業務内容、委託先の事業者名と管理責任者を利用者に公開している
☐	個人情報を取り扱う業務が再委託されている場合、再委託内容、委託先における再委託先への監督にかんする事項を確認し、必要最小限の再委託としている
☐	委託先に渡す個人情報は、委託する業務に必要な範囲に設定している
☐	委託契約終了後あるいは個々の委託事業終了ごとに、その個人データを返却する確認書をとっている
☐	廃棄処分とする場合には廃棄する事業者名、管理責任者名を確認し、破棄証明書をもっている

【第三者提供と共有化】

☐	利用目的に第三者提供が明示されている
☐	個人データの第三者提供には原則として本人の同意を要することを規定などにより従業員に周知している
☐	第三者提供の制限とその例外に該当する事例について、従業員に正しく周知している
☐	患者・利用者の状況を家族に説明する場合にも、原則として利用者の同意が必要であることを、規定などにより従業員に周知している
☐	第三者提供に関して電話や口頭で同意を得た場合には、その旨を記録している
☐	事例検討会等で個人データを利用する場合には、個人が特定されないように匿名化や検討内容に影響しない範囲での記述の変更などを行っている

☐	サービス担当者会議において利用者の個人情報を共有化するにあたり、個人情報の保護と守秘義務の徹底を図っている
--------------------------	---

【開示などの手続き】

☐	本人・代理人からの保有個人データ開示などの受付窓口を設置し、利用者に分かるように公表している
☐	本人・代理人からの開示等に関する手続きを書いた従業員向けの手引きを整備している
☐	本人・代理人からの開示などに関する手続きを書いた従業員向けの開示規定を整備している
☐	本人・代理人が開示などを申請するための様式類を整備している
☐	開示などの申請に対し、受け付けた受領書を整備している
☐	どのような場合に非開示となるかについて開示規定等により従業員に正確に周知している
☐	開示・非開示などの判断を組織的に行う体制を整えている
☐	開示などを求める本人・代理人の確認手続き、代理権の確認手続きを開示規定類に適切に定めている
☐	開示方法は本人・代理人に配慮し、来所・訪問・郵送など選択できるようになっている
☐	開示手数料は実費を勘案し、合理的な範囲内の金額になっている

【相談、苦情対応など】

☐	個人情報に関する相談や苦情解決の窓口を設置している
☐	個人情報に関する区校解決の手続きを定めている
☐	相談、苦情の申し出のために記入する様式を整備している
☐	苦情解決の担当者を決めている
☐	相談や苦情にあたり、利用者や家族が相談しやすい環境作りを行っている
☐	事業所内への掲示やホームページへの掲載によって、草案や苦情解決の窓口が患者・利用者などに周知されるよう努めている
☐	利用者からの問い合わせ、相談、苦情が個人情報の取り扱いの改善のための有益な資料として活用されるような意識と組織の体制になっている
☐	保有個人データに関する事項について問い合わせがあった場合、遅滞なく具体的な対応ができる体制が整っている

【公表等の方法】

☐	事業所内に掲示する際は受付窓口近くなどのみやすい場所に、見やすい大きさの文字で掲示している
☐	ホームページに公表している場合、基本方針、利用目的において保有個人データの取り扱い事項、共同利用に関する事項などを明示している
☐	利用契約書または重要事項説明書に、個人情報の基本方針、利用目的、取扱い、相談・苦情解決窓口などの項目及び説明を記述している

チェックリストにある項目はどれも個人情報保護の上で必要不可欠な項目であり、達成することが望ましいと考えられます。まずは職員教育の一環としてチェックリストを従業員間で共有し、リスクアセスメントや対策に活用し、可能な項目から実施ください。

<出典>

1. 2014年度情報セキュリティインシデントに関する調査報告書～個人情報漏洩編～ 第1版
NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ
2. 独立行政法人情報処理推進機構セキュリティセンター
IPA対策のしおり、情報漏洩発生時の対応ポイント集