「プライバシーマーク制度における要求事項」との対応表（認定指針第５版対応）

「対応するPMSの規程・様式の名称と項番」の記述内容については記入例を示しています

（申請事業者の内部規程・様式がプライバシーマーク制度における要求事項（認定指針第５版対応）の全項目に対応していることを示すと共に、審査時には添付の規程類の索引として使用します。）記入方法の詳細については以下をご参照ください

**【記入上の注意】**

1. A4縦の用紙をご使用ください。

2. 構築したPMS文書の内容と「プライバシーマーク制度における要求事項」の内容を比較し、「対応するPMSの規程・様式の名称と項番」に、対応するPMSの名称・項番（対応箇所）をご記入ください。本ポイントは審査で必ず確認する事項なので、漏れがあるなら必要に応じてPMSにご反映ください。

3. 「プライバシーマーク制度における要求事項」の内容：

* プライバシーマーク制度における要求事項は番号（J～）、ポイントは”①～”で表示しています。
* 各項目のポイント①～は、原則保健医療福祉分野のプライバシーマーク認定指針第５版のC.最低限のガイドラインに対応しています。
* ポイントはPMSを構築する上での具体的な留意点です。
* ポイントは事業者の業種、規模により異なるため、必ずしも全てを満たす必要はありません。
* ポイントで”～している”という項目において､実例がある場合は該当する様式名・規定等を記入し、実例が無い場合は”実例なし”と記載することで可｡
* ポイントは必要に応じ随時見直しを実施します。

4. 「対応するPMSの規程・様式の名称と項番」の記入方法：

* プライバシーマーク制度における要求事項の全項目およびポイントについて、対応するPMSの規程名称及び項番（対応箇所）を記入してください。対応する規程が複数ある場合は、個人情報保護マネジメントシステム（PMS）文書の体系に合わせて階層的にご記入ください。
* ポイントへの対応は、項番（①など）と対応させ、対応関係を明確にしてください。
1. グレーの網掛けについては、該当する規定がない場合は記述する必要はありません

※網掛けの項目は、現地審査での確認事項となります（トップインタビューでの確認事項）

※個人情報基本規程等に網掛けの項目に該当する規定がある場合は、対応するPMSの規程名称及び項番（対応箇所）を記入してください。

1. 「使用する様式」の記入方法
* 「対応するPMSの規程・様式の名称と項番」で記入した項に基づく運用のための様式があれば、その名称も必ずご記入ください。

**【トップインタビューでの主な確認内容】**

**※各審査項目のうち網掛け部分【トップインタビューでの確認事項】については、以下の内容をトップインタビューで確認させていただきます**

|  |  |
| --- | --- |
| 項目 | 主な確認内容 |
| 個人情報保護の目的について | ・P マークの取得を目指す具体的な理由を、自社の事業との関係と共に説明していただきます 。・個人情報保護の目的を達成するためのPMS に関連する利害関係者にはどのような者や組織があり、それらの要求事項にはどのようなものがあるのかを説明していただきます 。 |
| 個人情報保護方針について | ・個人情報保護方針は、個人情報の取扱い（適切な取得・利用・提供に関すること、安全管理措置を徹底すること、苦情相談窓口を設けること等）に関して、対外的に約束するものですが、その個人情報保護方針はどのような手順で策定し、事業者内部及び外部へどのように周知している（入手可能な措置を講じている）かを説明していただきます。 |
| 個人情報保護のための資源について | ・PMSを運用するために、どのような役割が必要と考え、責任及び権限を与えたのか、また、どの従業者に割り当てているのかを説明していただき ます。・役割を割当てた従業者に対して、トップマネジメントとしてどのような支援しているか（役割を割り当てた担当者からの報告・相談等への対応など）説明していただきます 。 |
| マネジメントレビューについて | ・マネジメントレビューの結果を踏まえて、改善が必要だと考えているところがあるか（どのような問題点があり、どのように対応を指示したのか、または今後どのように対応しようとしているのか）を説明していただきます。 |
| PMSの継続的な改善について | ・これまでのPMSの変更状況や、今後もPMSの見直しを行うことについて確認させていただきます。 |

＊個人情報保護マネジメントシステムはPMSと略記する

**＊緑色の記述は記入例です。記入時は緑色の記述を削除の上、記入してください**

| プライバシーマーク制度（認定指針）における要求事項とポイント | 対応するPMSの規程・様式の名称と項番 |
| --- | --- |
| **1 （J.1.4）　適用範囲**1. 自らの事業の用に供している全ての個人情報の取扱いを個人情報保護マネジメントシステムの適用範囲と定める旨が文書化されている
 | 個人情報保護規程第1条 |
| 1. 文書化した情報は利用可能な状態にしている
 | 社内イントラで参照・各部署へ紙で配布 |
| 1. 保護の対象は従業者に関する個人情報や採用情報も対象としている
 | 個人情報保護規程第1条 |
| 1. PMSを運用する従業者の範囲を明確にしている（パート、アルバイト、派遣職員、実習生、ボランティアなども含めている）
 | 個人情報保護規程第1条 |
| **２　用語及び定義** |  |
| **J.1組織の状況** |  |
| **J.1.1　組織及びその状況の理解**①個人情報を取り扱う事業に関して、個人情報保護マネジメントシステムに影響を与えるような外部及び内部の課題を特定している | 個人情報保護規程第2条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.1.2　利害関係者のニーズ及び期待の理解**①a)～b)を特定しているa)個人情報保護マネジメントシステムに関連する利害関係者 b)その利害関係者の、個人情報保護に関連する要求事項 | 個人情報保護規程第3条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.1.3　法令、国が定める指針及びその他の規範**1. 参照している規格、法令等が明確である（名称、バージョン、発行日、発行者、URL）
 | 個人情報保護規程第4条法令等管理台帳 |
| 1. 個人情報の取扱いに関する法令、国が定める指針その他の規範（以下、“法令等”という）を特定し参照できる手順が内部規程として文書化されている
 | 個人情報保護規程第4条 |
| 1. 見直し時期が明確である（少なくとも半年以内）
 | 個人情報保護規程第4条 |
| 1. 参照している規格、法令等が改廃された場合、可及的速やかにPMSや関連内規などにその改廃内容を反映する手順を定めている
 | 個人情報保護規程第4条 |
| 1. 認定指針J.1.3に例示する法令等が含まれている

※認定指針に示すＧＬ等は例示であり、各事業者で業務に応じて必要となるＧＬ等を特定すること（緑字は必須）a)JIS Q 15001（＋プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針）b)保健医療福祉分野のＰマーク認定指針c)個人情報の保護に関する法律d)個人情報の保護に関する法律施行令e)個人情報の保護に関する法律施行規則f)個人情報の保護に関する法律についてのガイドライン（通則編)g)同ガイドライン（第三者提供時の確認・記録義務編)h)同ガイドライン（外国にある第三者への提供編)i)同ガイドライン（仮名加工情報・匿名加工情報編)j)雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項k)医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスl)医療情報システムの安全管理に関するガイドラインm)医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドラインn)診療情報の提供等に関する指針o)医療分野の研究開発に資するための匿名加工医療情報に関する法律p)心理的な負担の程度を把握するための検査及び面接指導の実施並びに面接指導結果に基づき事業者が講ずべき措置に関する指針q)行政手続における特定の個人を識別するための番号の利用等に関する法律r)特定個人情報の取扱いに関するガイドライン(事業者編)s)民間PHR事業者による健診等情報の取扱いに関する基本的指針t)オンライン診療の適切な実施に関する指針 | 法令等管理台帳でa)～t)を特定している |
| **J.1.4　個人情報保護マネジメントシステムの適用範囲の決定**①自らの事業の用に供している全ての個人情報の取扱いを個人情報保護マネジメントシステムの適用範囲とする旨が文書化されている | ―【記入上の注意】本項目は1 （J.1.4）　適用範囲で対応するため記入不要です |
| **J.1.5　個人情報保護マネジメントシステム**①本指針に従って、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、継続的に改善している | 個人情報保護規程第5条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.2リーダーシップ** |  |
| **J.2.1リーダーシップ及びコミットメント**①トップマネジメントは、a)～ h)について統率し、その結果について責任を持っている | 個人情報保護規程第6条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.2.2　個人情報保護方針**1. 事業者の業務に適した個人情報保護の理念が明確（“人格尊重の理念”が読みとれる）
 | 個人情報保護方針 |
| 1. 個人情報保護方針を文書化した情報に、2 項のa)～h)に定める事項が含まれている
 | 個人情報保護方針 |
| 1. ホームページに掲載する場合、PMS中の原本と同一のものが、単独のページとしてトップページおよび各ページから参照できる
 | 個人情報保護方針https;//aaa.ne.jp/privacy policy |
| 1. 個人情報保護方針の従業者（利害関係者も含む）が入手可能な措置、一般の人が入手可能な措置を講じている
 | 個人情報保護規程第７条 |
| **J.2.3.1　組織の役割、責任及び権限**①個人情報保護に関連する役割に対して、責任及び権限を割り当てて、その結果を利害関係者へ周知している | ～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| ②担当者の役割、及び役割に対する責任及び権限が内部規程として文書化されている | 個人情報保護規程第8条 |
| ③周知のため個人情報保護体制を一覧できる体制図を作成している | 個人情報保護体制図 |
| ④電子カルテ等の情報システムを導入している場合は、システム管理者を選任している | 個人情報保護体制図 |
| **J.2.3.2　個人情報保護管理者と個人情報保護監査責任者**① 個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、トップマネジメントに個人情報保護マネジメントシステムの運用状況を報告する旨が内部規程として文書化されている | 個人情報保護規程第8条 |
| ②個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、トップマネジメントに報告する旨が内部規程として文書化されている | 個人情報保護規程第8条 |
| ③監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保する旨が内部規程として文書化されている | 個人情報保護規程第8条 |
| ④個人情報保護管理者と個人情報保護監査責任者とは異なるものであること | 個人情報保護体制図 |
| ⑤医療機関では個人情報保護管理者は、法令で守秘義務が定められている職種の従業者から選任している | 院長を選任している |
| **J.2.4 管理目的及び管理策（一般）**1. J.1からJ.11の管理策について、定めた手段に従って承認されていること又は、承認のために定めた手段が説明できること

※J.1からJ.11の管理策についての承認手順が、本管理策で規定されている、もしくはJ.1からJ.11の管理策毎に承認手順が規定されていること（稟議規定等のPMS以外の規定おいて承認の手順が明確となっていることでも可） | 1. 個人情報保護規程第1条～28条
 |
| **J.3.1.1 個人情報の特定**1. 個人情報の特定のための具体的手順（５W1Hの観点）を規定している
 | 個人情報保護規程第8条個人情報特定・リスク分析規程I |
| ②個人情報の特定で使用する様式（「個人情報取扱申請書」等）がある | 個人情報取扱申請書 |
| ③個人情報を管理するための台帳を整備している | 個人情報管理台帳 |
| ④台帳には少なくとも以下の項目が含まれている* 個人情報の名称
* 件数（概数）
* 個人情報の項目
* 利用目的
* 保管方法
* 保管場所
* アクセス権を有する者
* 委託や提供の有無
* 廃棄方法
* 保有個人データ（開示対象であるか否か）の識別
* 利用期限
* 保管期限
 | 個人情報管理台帳 |
| ⑤新たに個人情報の取り扱いが発生した場合や、特定内容に変化があった場合の管理台帳への反映手順を明確に規定している | 個人情報特定・リスク分析規程I個人情報取扱申請書 |
| ⑥台帳の内容を少なくとも年一回、及び必要に応じて適宜に確認し、最新の状態で維持している | 個人情報特定・リスク分析規程I個人情報管理台帳 |
| ⑦全ての個人情報に（見直し時期という観点でも可）保管期限を定めている | 個人情報管理台帳 |
| ⑧保有個人データ（開示対象であるか否か）が識別されている | 個人情報管理台帳 |
| ⑨事業の用に供している匿名加工情報、仮名加工情報、個人関連情報を取り扱っている場合は、同様に（特定を）実施している | 個人情報管理台帳 |
| **J.3.1.2　 リスク及び機会に対処する活動**①個人情報保護マネジメントシステムの計画の策定にあたって、J.1.1 で把握した課題及び J.1.2 で特定した要求事項を考慮し、a)～c)を実現できるよう個人情報保護リスクアセスメント及び個人情報保護リスク対応をしている | 個人情報保護規程第9条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.3.1.3　個人情報保護リスクアセスメント**1. J.3.1.1によって特定した個人情報の取り扱いについて、個人情報保護リスクを特定し、分析し、必要な対策を講じる手順が内部規程として文書化されている（リスクの定期的見直し手順を含む）
 | 個人情報保護規程第10条個人情報特定・リスク分析規程Ⅱ |
| ②業務フロー等を活用し、特定した各個人情報のライフサイクルに応じたリスク分析を実施している | 個人情報特定・リスク分析規程Ⅱリスク分析表 |
| ③リスクに応じた対策が明確である（対策はPMSに反映されている | 個人情報特定・リスク分析規程Ⅱリスク分析表 |
| ④未対応部分を残留リスクとして把握し、管理している | 個人情報特定・リスク分析規程Ⅱリスク分析表 |
| ⑤特に要配慮個人情報を取り扱う部門においては、残留リスクを分析し、その後の対応を明確にしている（パフォーマンス評価（J.6）に反映されている） | リスク分析表運用点検表（各部門） |
| ⑥「個人情報取扱申請書」等により、取扱の新規・変更時にリスク分析を実施する手順がある | 個人情報特定・リスク分析規程Ⅱリスク分析表 |
| ⑦定めた手順及び実施した内容については、少なくとも年一回、及び必要に応じて適宜に見直している | 個人情報特定・リスク分析規程Ⅱリスク分析表 |
| ⑧文書化した情報は利用可能な状態にしている | 個人情報取扱申請書リスク分析表 |
| **J.3.2　個人情報保護目的及びそれを達成するための計画策定**①a)～e)を含めて、個人情報保護目的を達成するために計画しているa)実施事項b)必要な資源c)責任者d)達成期限e)結果の評価方法 | 個人情報保護規程第11条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.3.3　計画策定**1. 教育計画書の立案と承認及び維持管理の具体的手順が内部規程として文書化されている（5W1Hの観点）
 | 個人情報保護規程第12条PMS教育規程第4条 |
| ②年間教育計画書、個別教育計画書（詳細計画書）がある(個別計画は望ましい事項) | PMS教育年間計画書PMS教育部門計画書 |
| ③監査計画書の立案と承認及び維持管理の具体的手順が内部規程として文書化されている（5W1Hの観点） | 個人情報保護規程第12条PMS監査規程第4条 |
| ④年間監査計画書、個別監査計画書（詳細計画書）がある(個別計画は望ましい事項) | PMS監査年間計画書PMS監査部門計画書 |
| **J.3.4 変更の計画策定**１．事業者は、個人情報保護マネジメントシステムの変更の必要性に関する決定をしたとき、その変更を計画している | ～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.4　支援** |  |
| **J.4.1　資源**①個人情報保護マネジメントシステムの確立、実施、維持及び継続的改善に必要な資源を決定・確保し、利害関係者へ提供している | 個人情報保護規程第13条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.4.2　力量**①a)～d)を行っている | 個人情報保護規程第14条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.4.3　認識**1. 全ての従業者に対して、少なくとも年一回、及び必要に応じて適宜に教育を実施する手順（教育の理解度を確認する手順を含む）が内部規程として文書化されている
 | 個人情報保護規程第15条PMS教育規定第1条 |
| ②教育対象には、直接雇用関係のある従業者のみならず、取締役、執行役、理事、監査役、監事、派遣職員等も含むことが明確（非常勤の理事等の場合は、少なくともテキスト配布するなどの措置を講じている） | PMS教育規程第2条 |
| ③全ての従業者に対して、J.4.3のa)～d)の内容を認識させている | 20××年度教育テキスト教育出欠名簿20××年教育実施報告書 |
| ④受講者の理解度確認を実施している | 小テストで理解度確認を実施 |
| ⑤欠席者や不合格者へのフォローアップを実施している | 20××年度教育テキスト教育出欠名簿20××年教育実施報告書 |
| ⑥事故が発生している場合は、再発防止策及び事故の発生原因などを従業者に教育している | 20××年度教育テキスト個人情報に関する事故について（経緯及び再発防止策）（社内周知文） |
| **J.4.4.1　コミュニケーション**①個人情報マネジメントシステムを構築・運用するにあたり、a)～f)を考慮して、内外の利害関係者と意思疎通や情報共有を行っている | 個人情報保護規程第16条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.4.4.2　緊急事態への準備**①個人情報保護リスクを考慮し、その影響を最小限とするため、緊急事態を特定するための手順、及び特定した緊急事態にどのように対応するかの手順が内部規程として文書化されている | 個人情報保護規程第16条緊急事態対応規程第4条 |
| ②緊急事態への準備及び対応に関する規定には、緊急事態が発生した場合に備え、J.4.4.2 のa)～c)の事項を含む対応手順が含まれている | 緊急事態対応規程第5条緊急事態報告先一覧 |
| ③関係機関への報告に際して、具体的な報告先（担当部署、電話番号、メールアドレス、URLなど)を事前に調査しておくことまた、保健医療分野のプライバシーマークを取得している事業者は（申請準備中、申請中を含む)、指定審査機関である(一財)医療情報システム開発センターへの報告手順も規定している | 緊急事態対応規定第5条緊急事態報告先一覧 |
| ④緊急事態への準備のための①～③の手順については、①及び②を踏まえたうえで、5W1Hの観点で、以下の具体的手順がある１）実態の把握と応急処置２）緊急連絡（緊急連絡網）３）速やかに本人及び関係者に通知４）事実関係等を遅滞なく公表５）MEDIS-DC他、関係機関に直ちに報告６）本人への謝罪７）再発防止策を検討し実施８）監査（臨時監査）を実施し確認 | 緊急事態対応規程第5条緊急事態報告先一覧 |
| ⑤緊急事態が発生した場合，定めた手順に従って緊急事態への対応を実施している | 緊急事態対応報告書 |
| **J.4.5.1　文書化した情報**①個人情報保護マネジメントシステムの基本となるJ.4.5.1 のa)～f)の要素に対応する書面があるa)個人情報保護方針b)内部規程c)内部規程に定める手順上で使用する様式d)計画書e)本指針が要求する記録f)その他、事業者が個人情報保護マネジメントシステムを実施する上で必要と判断した文書（記録を含む） | 個人情報保護規程第17条1. 個人情報保護方針
2. 個人情報保護規程、各下位規程・マニュアル（PMS文書管理台帳）
3. 各様式類（PMS記録管理台帳）
4. 教育・監査計画書（年間、部門別）
5. PMS記録管理台帳
6. PMS文書管理台帳/ PMS記録管理台帳
 |
| **J.4.5.2　文書化した情報の管理**①文書化した情報は、J.4.5.2のa)～f)の事項を満たしているa)文書化した情報が、必要な時に、必要な所で、入手可能かつ利用に適した状態である b)文書化した情報が十分に保護されている(例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護) c)配付、アクセス、検索及び利用 d)読みやすさが保たれることを含む、保管及び保存 e)変更の管理（例えば、版の管理） f)保持及び廃棄 | 個人情報保護規程第18条1. 社内イントラで参照
2. アクセス制限（外部アクセス不可）
3. 社内イントラで参照
4. 社内イントラで参照
5. 各規程に改訂履歴を記載

文書管理台帳1. 規定に基づき保持・廃棄
 |
| ②個人情報保護マネジメントシステムに必要となる外部からの文書化した情報は、必要に応じて特定し、管理している　※例：委託元から示された作業指示書等が該当 | PMS文書管理台帳 |
| **J.4.5.3　文書化した情報（記録を除く）の管理**①本指針が要求する全ての文書化した情報（記録を除く）を管理する手順が内部規程として文書化され、J.4.5.3のa)～d)の事項が含まれている（発行、改訂、保管、破棄等の手順が規定されている）　a)文書化した情報（記録を除く）の発行及び改正に関することb)文書化した情報（記録を除く）の改正の内容と版数との関連付けを明確にすることc)必要な文書化した情報（記録を除く）が必要なときに容易に参照できることd)適切性及び妥当性に関する、適切なレビュー及び承認を行うこと | 個人情報保護規程第18条 |
| ②文書化した情報(記録を除く)の管理を実施している | PMS文書管理台帳 |
| **J.4.5.4　内部規程**1. J.4.5.4 のa)～o)の事項を含む内部規程が文書化されている
 | 個人情報保護規程第19条 |
| ②事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改正している | PMS文書管理台帳個人情報保護規程各下位規程・マニュアル |
| ③医療情報システム（保健医療福祉分野の個人情報を取り扱うシステム）を導入している場合、厚生労働省の定める運用管理規程を定めているまたは医療情報システムの安全管理に関するガイドラインの要求事項については、ＰＭＳ全体で担保することを明確にしている | 個人情報保護規程第19条 |
| **J.4.5.5　文書化した情報のうち記録の管理**1. 個人情報保護マネジメントシステム及び本指針で要求されている記録の管理についての手順が内部規程として文書化されている
 | 個人情報保護規程第20条 |
| ②J.4.5.5 のa)～kの事項を含む必要な記録を作成しているa)法令、国が定める指針及びその他の規範の特定に関する記録b)個人情報の特定に関する記録c)個人情報保護リスクアセスメント及び個人情報保護リスク対応に関する記録d) 次の事項を含む管理策で要求する記録1）利用目的の特定に関する記録2）保有個人データに関する開示等（利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止又は消去，第三者提供の停止）の請求等への対応記録3）第三者提供に係る記録4）第三者提供に関する開示等の請求等への対応記　　録5）個人情報の適正管理への対応記録e) 教育などの実施記録f) 苦情及び相談への対応記録g) 緊急事態への対応記録h) 監視、測定、分析及び評価の記録i) 内部監査の記録j) マネジメントレビューの記録k) 不適合及び是正処置の記録 | PMS記録管理台帳a)法令等管理台帳b)個人情報管理台帳c)リスク分析表d) 次の事項を含む管理策で要求する記録1）個人情報管理台帳2）開示等対応記録3）第三者提供記録簿4）開示等対応記録5）各記録類e) 教育実施報告書f) 苦情相談対応記録g) 緊急事態対応報告書h) 運用点検簿（各部門）i) 内部監査報告書j) マネジメントレビュー報告書k) 不適合報告書 |
| **J.5　運用** |  |
| **J.5.1　運用**1. 個人情報保護マネジメントシステムを確実に実施するために、運用の手順が内部規程として文書化されている
 | 個人情報保護規程第21条 |
| ②本指針の要求事項を満たすため、及び J.3 で決定した活動について、計画し、実施し、管理している | 各PMS運用記録 |
| ③計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとっている | 各PMS運用記録 |
| ④外部委託した業務がある場合は、管理の対象としている | 委託先一覧表、委託先評価表 |
| ⑤②～⑤の記録を保持している | 各PMS運用記録 |
| **J.6　パフォーマンス評価** |  |
| **J.6.1　監視、測定、分析及び評価**1. 各部門及び階層の管理者が定期的に、及び適宜にマネジメントシステムが適切に運用されていることを確認する手順が内部規程として文書化されている
 | 個人情報保護規程第22条１項 |
| ②特に要配慮個人情報を取り扱う部門においては、リスクアセスメント（J.3.1.3）の結果、認識した残留リスクについて、その対応をチェックリスト等に反映し、定期的に実施状況を確認することにより残留リスクを低減する措置を講じている | PMS運用チェックリスト |
| ③個人情報保護マネジメントシステムが適切に運用されているかどうかを確認するために、a)～f)の事項を決定している | PMS運用チェックリスト |
| ④運用の確認のためのチェックリストがある | PMS運用チェックリスト |
| ⑤少なくとも以下の確認した記録を残す規定がある1. 最終退出時の社内点検（施錠確認等）
2. 入退館（室）の記録の定期的な確認
3. アクセスログの定期的な確認
 | 個人情報保護規程第22条2項 |
| ⑥運用の確認を実施している | PMS運用チェックリスト部門入退記録簿アクセスログ記録簿 |
| ⑦運用の確認において、不適合が確認された場合は、是正処置を行っている | 是正処置実施記録 |
| ⑧個人情報保護管理者は、定期的に、及び適宜にトップマネジメントに運用の確認状況を報告する手順を規定し、報告している | 個人情報保護規程第22条１項マネジメントレビュー記録等 |
| ⑨監視及び測定の結果の証拠となる、文書化した情報を利用可能な状態にしている | PMS運用チェックリスト部門入退記録簿アクセスログ記録簿 |
| **J.6.2　内部監査**1. 内部監査の計画及び実施、結果並びにこれに伴う記録の保持に関する責任及び権限を定める手順が内部規程として文書化されている
 | 個人情報保護規程第23条PMS内部監査規定第1条～5条 |
| ②内部監査実施計画（J.3.3 b))に従って、事業者の内部規程が、本指針の要求事項に適合していること（適合状況）、及び個人情報保護マネジメントシステムが有効に実施され、維持されているか（運用状況）について、少なくとも年一回、及び必要に応じて適宜に内部監査を実施している | 内部監査計画書内部監査報告書内部監査チェックリスト（適合性監査）内部監査チェックリスト（運用監査） |
| ③監査人は、自ら所属する部門を内部監査しないように規定されている | PMS内部監査規定第6条 |
| ④内部監査結果の報告は、個人情報保護監査責任者からトップマネジメントに行っている | 内部監査報告書 |
| ⑤全部門の監査が実施されている | 内部監査計画書内部監査報告書内部監査チェックリスト（運用監査） |
| ⑥内部監査実施計画及び内部監査結果の証拠となる、文書化した情報を利用可能な状態にしている | 内部監査計画書内部監査報告書内部監査チェックリスト（適合性監査）内部監査チェックリスト（運用監査） |
| **J.6.3　マネジメントレビュー**1. マネジメントレビューを実施する手順が内部規程として文書化されている
 | 個人情報保護規程第24条 |
| ②マネジメントレビューを実施するにあたり、J.6.3のａ）～ｆ）の事項がインプットされている | マネジメントレビュー実施記録 |
| ③運用状況に関する報告には、事故、ヒヤリハット等の発生状況や発生時の対応状況等の報告も含まれる。漏れなく報告されるようにしている | 個人情報保護規程第第24条マネジメントレビュー実施記録 |
| ④少なくとも年一回、及び必要に応じて適宜にマネジメントレビューを実施している | マネジメントレビュー実施記録 |
| ⑤マネジメントレビューのアウトプット（記録）を残している（マネジメントレビューのアウトプットには、継続的改善の機会及び個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定を含んでいる） | マネジメントレビュー実施記録 |
| ⑥マネジメントレビューの結果の証拠となる、文書化した情報は利用可能な状態にしている | マネジメントレビュー実施記録 |
| **J.7 改善** |  |
| **J.7.1不適合及び是正処置**1. 不適合に対する是正処置を確実に実施するための責任及び権限を定める手順が内部規程として文書化され、J.7.1 のa)～e)の事項が含まれている
 | 個人情報保護規程第25条 |
| 1. 是正処置実施のための手順には、認定指針に示す以下の点にも留意している
2. 不適合の内容を承認するのはトップマネジメントである
3. 不適合の原因を特定し、是正処置案を立案するのは、不適合が発見された部門である
4. 立案された是正処置案を承認（指示）するのはトップマネジメントである
5. 監査責任者は、独立性の観点から改善案の立案・承認に関与しない（有効性のレビューは除く）
 | 個人情報保護規程第25条 |
| ③緊急事態への準備(J.4.4.2)、苦情及び相談への対応（J.11.1)、監視、測定、分析及び評価(J.6.1)、内部監査(J.6.2)又は外部機関の指摘等により発見された不適合を改善するための手順をａ)～ｅ)に則って定めるとともに承認、及び記録する手順・様式を整備している | 個人情報保護規程第25条是正処置実施記録 |
| ④不適合が明らかになった場合、J.7.1 のa)～e)の事項を実施している | 是正処置実施記録 |
| ⑤J.7.1 のa)～e)の実施結果について、文書化した情報を利用可能な状態にするとともに、原則として、トップマネジメントが承認している | 是正処置実施記録マネジメントレビュー実施記録 |
| **J.7.2 継続的改善**①個人情報保護マネジメントシステムの適切性、妥当性及び有効性を継続的に改善している | 個人情報保護規程第26条～トップインタビューでの確認事項～【記入上の注意】5（赤字）及び【トップインタビューでの主な確認内容】をご参照ください |
| **J.8　取得、利用及び提供に関する原則** |  |
| **J.8.1　 利用目的の特定**1. 個人情報の利用目的をできる限り特定し、その目的の達成に必要な範囲内において取り扱いを行なっている（通知又は公表の記録、本人に明示した書面（同意書）に記載された利用目的が、J.3.3.1で特定した利用目的の範囲内である）
 | 個人情報保護規程第27条個人情報管理台帳利用目的公表文書各同意書 |
| 1. 利用目的は、取得した情報の利用及び提供によって本人の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにしている（個人情報管理台帳、通知文・同意文書で利用目的を明確にしている）
 | 個人情報保護規程第27条個人情報管理台帳利用目的公表文書各同意書 |
| **J.8.2　適正な取得**1. 定めた手順に従って、適法かつ公正な手段によって個人情報を取得していること（J.4.5.4に該当する規程に基づき個人情報を取得している）
 | 個人情報保護規程第28条利用目的公表文書各同意書 |
| ②当該患者等以外の情報を患者等から得る場合は、その情報の必要性を十分検討した後に行い、取得された情報の利用は当該患者等の診療遂行に必須のものに限定することを規定している | 個人情報保護規程第28条各同意書 |
| ③説明による同意が困難な場合（意識障害、精神障害、乳幼児など）診療の遂行上の必要性を十分検討し、必要性を記録した上で情報の取得を行うことを規定している | 個人情報保護規程第28条各同意書 |
| ④親権者、保護者が定まっている場合はその了承を可能な限り得るように規定している | 個人情報保護規程第28条各同意書 |
| **J.8.3　要配慮個人情報**1. 要配慮個人情報（性生活、性的指向又は労働組合に関する情報を含む）の取得に際しては、要配慮個人情報の取得、利用、又は提供（要配慮個人情報のデータの提供含む）する旨について、あらかじめ書面によって明示し、書面によって本人の同意を得ている
 | 個人情報保護規程第29条・個人情報同意書（診療）・個人情報同意書（介護）・個人情報同意書（健診）・個人情報同意書（予防接種） |
| ②要配慮個人情報を取得する際に本人の同意を要しない場合、J.8.3 のただし書きa)-k)の場合に限定している | 個人情報保護規程第29条 |
| ③個人情報に、性生活、性的指向又は労働組合に関する情報が含まれる場合には、当該情報を要配慮個人情報と同様に取り扱う旨が文書化されている | 個人情報保護規程第29条 |
| ④J.8.3 の a)～k)を適用してあらかじめ書面による本人の同意を得ずに要配慮個人情報を取得する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報保護規程第29条個人情報取扱申請書（実績無し） |
| **J.8.4 個人情報を取得した場合の措置**①利用目的を通知・公表する方法が明確 | 個人情報保護規程第30条 |
| ②個人情報を取得した場合、個人情報の取得の場面に応じて、あらかじめ、その利用目的を公表している場合を除き、取得後速やかにその利用目的を本人に通知し、又は公表している | 利用目的公表文書（当法人の利用目的について） |
| ③本人への利用目的の通知又は公表を要しないのは、J.8.4 の a)～d)の場合に限定しているa)利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合b)利用目的を本人に通知し、又は公表することによって当該事業者の権利又は正当な利益を害するおそれがある場合c)国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがある場合d)取得の状況からみて利用目的が明らかであると認められる場合 | 個人情報保護規程第30条 |
| ④J.8.4 の a)～d)を適用して本人に対し個人情報の利用目的の通知又は公表をしない場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報取扱申請書（実績無し） |
| ⑤保健医療福祉分野における個人情報の取得は、要配慮個人情報を取得することから、本人から直接書面で取得する場合以外でも、”本人から直接書面で取得する場合”の措置に準じた明示的同意を得ることを原則とすることを明確にしている | 個人情報保護規程第30条 |
| **J.8.5　J.8.4のうち本人から直接書面によって取得する場合の措置**1. 個人情報を直接書面によって取得する場面（業務）毎に、明示・同意の方法、様式等の手順を定めている(5W1Hの観点）
 | 個人情報保護規程第30条 |
| ②取得場面毎に同意に用いる様式を整備している | 個人情報同意書（診療）個人情報同意書（介護）個人情報同意書（健診）個人情報同意書（予防接種）個人情報同意書（採用応募時）個人情報同意書（採用時）Webフォーム（お問合せ等） |
| ③チェック方式とするなら「同意する」、「同意しない」、または「一部不同意」等の選択肢を設けている（診療の場合） | 個人情報同意書（診療） |
| ④従業者（募集時、採用時）に対しても本措置を実施する旨が明確である | 個人情報保護規程第30条個人情報同意書（採用応募時）個人情報同意書（採用時）Webフォーム（募集） |
| ⑤ホームページから取得する場合の措置（同意、暗号化等）を規定している | 個人情報保護規程第30条個人情報同意書（採用応募時）個人情報同意書（採用時）Webフォーム（お問合せ等） |
| 1. あらかじめ書面によって本人に明示し、書面によって本人の同意を得ないのは、以下の場合に限定していること
* 人の生命、身体若しくは財産の保護のために緊急に必要がある場合
* 利用目的を本人に通知するか、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
* 利用目的を本人に通知するか、又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合
* 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的 を本人に通知するか、又は公表することによって当該事務の遂行に支障を及ぼすおそれがある場合
* 取得の状況からみて利用目的が明らかであると認められる場合
 | 個人情報保護規程第30条 |
| ⑦J.8.5の2項のただし書きを適用する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報保護規程第30条個人情報取扱申請書 |
| ⑧意識障害、精神障害、乳幼児などで、本人に理解能力がない場合で、親権者や保護者が定まっている場合は可能な限り親権者や保護者に提示し同意を得ることを定めている | 個人情報保護規程第30条個人情報同意書（診療）個人情報同意書（介護） |
| ⑨同意を得る際には、患者等が個人情報の利用目的に応じて、個別に拒否できるオプションを用意し、その際の対応手順を規定している | 個人情報保護規程第30条個人情報同意書（診療） |
| ⑩健診事業において、精密検査などの２次健診等を他の医療機関等へ紹介した場合で、紹介先の医療機関等から受診者の検査結果を受領した場合、同意書等であらかじめ書面による本人の同意を取得している | 個人情報保護規程第30条個人情報同意書（健診） |
| **J.8.6　利用に関する措置**1. 本措置を実施するための手順（同意取得手順）が文書化されている。事例がないなら、その旨を明確にし、禁止している
 | 個人情報保護規程第31条 |
| ②特定した利用目的の達成に必要な範囲内で個人情報を利用している | 個人情報保護規程第31条 |
| ③個人情報を利用する場合には、本人の同意の有無に関わらず、違法又は不当な行為を助長し、又は誘発するおそれのある利用をしていない | 利用していない |
| ④目的外利用に該当するかどうか判断に迷う場合、個人情報保護管理者の承認を求めるように規定している | 個人情報保護規程第31条 |
| ⑤（特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合に、）本人の同意を得ることを要しないのは、J.8.3のa)～f)のいずれかに該当する場合に限定している | 個人情報保護規程第31条 |
| ⑥J.8.6のa)～f)を適用して同意なしに特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報保護規程第31条個人情報取扱申請書 |
| ⑦学会発表等への利用について規定している | 個人情報保護規程第31条 |
| ⑧特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合は、あらかじめ、少なくとも、J.8.5のa)～f)又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得ている | 個人情報同意書 |
| **J.8.7　本人に連絡又は接触する場合の措置**1. 本措置を実施するための手順（同意取得手順）が文書化されている。事例がないなら、その旨を明確にし、禁止している
 | 個人情報保護規程第32条 |
| ②個人情報を利用して本人に連絡又は接触する場合には、本人に対して、J.8.5のａ)～ｆ)又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得ている | 個人情報同意書 |
| ③個人情報を利用して本人に連絡又は接触する場合のうち、本人に通知し、本人の同意を得ることを要しない場合は、 J.8.7 のa)～i)に限定して規定している | 個人情報保護規程第31条 |
| ④J.8.7 のa)～i)を適用を適用して同意なしに個人情報を利用して本人に連絡又は接触する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報取扱申請書 |
| ⑤健診業務等（ストレスチェック業務も含む）の要配慮個人情報の取り扱いを委託される場合は、あらかじめ書面による本人の同意を得ている | 個人情報同意書（健診） |
| **J.8.8　個人データの提供に関する措置** 1. 本措置を実施するための手順（同意取得手順）が文書化されている
 | 個人情報保護規程第33条 |
| ②個人データを第三者に提供する場合には、あらかじめ、本人に対して、J.8.5のa)～d)又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得ている | 個人情報同意書（各種） |
| ③個人データを第三者に提供する場合に、本人に通知し、本人の同意を得ることを要しない場合は、J.8.8 の a)～l)に限定して規定している | 個人情報保護規程第33条 |
| ④J.8.8 のa)～l)を適用して本人の同意なしに個人情報を第三者に提供する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報取扱申請書 |
| ⑤意識障害、精神障害、乳幼児などで同意を得ることが困難な場合の措置を規定している（虐待が疑われる場合は除く） | 個人情報保護規程第33条 |
| ⑥警察や検察等捜査機関からの照会や事情聴取があった場合の措置を規定している（所属確認手順、捜査関係事項照会書等の提出を求めるなど）※医療・健診等において要配慮個人情報についての照会を求められた場合 | 個人情報保護規程第33条 |
| ⑦健診の場合、法定外健診の事業者への結果報告の同意を得ていることを確認できる（契約等）または拒否できるような措置がとられている | 個人情報同意書（健診）健診委託契約書（委託元事業者へ法定健診結果を提供する場合は、委託元事業者側で本人同意を取得する旨を契約書に定めている） |
| ⑧調剤薬局の場合、代理人へ薬を渡す際の手順を規定している | 個人情報保護規程第33条個人情報同意書 |
| **J.8.8.1　外国にある第三者への提供の制限**1. 外国にある第三者に個人データを提供する場合、J.8.8.1のa）～ｃ）のいずれかを満たす旨が文書化されている
 | 1. 個人情報保護規程第34条
 |
| ②外国にある第三者に個人データを提供する場合、J.8.8.1のa）～ｃ）のいずれかを満たしていること | 1. 個人情報同意書
 |
| ③J.8.8.1 の a)～c)のいずれか以外で、 本人の同意を得ることを要しない場合は、J.8.8 のf)～l)のいずれかの場合に限定している | 1. 個人情報保護規程第34条
 |
| ④J.8.8 のf)～l)を適用する場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 1. 個人情報取扱申請書
 |
| ⑤J.8.8.1 の a)によって、外国にある第三者に個人データを提供する場合は、あらかじめ、 J.8.8.1 の d)～i)に掲げる事項についての情報を、当該本人に提供している | 1. 個人情報同意書
 |
| ⑥J.8.8.1 の b)によって外国にある第三者に個人データを提供する場合は、あらかじめ、 J.8.8.1 の j)～l)の事項について、必要な措置を講じている | 1. 第三者提供契約書
2. 業務委託契約書（委託の場合）
 |
| ⑦J.8.8.1 の l)で、本人の求めに係る情報の全部又は一部について提供しない旨の決定をしたときは、本人に対して、遅滞なく、その旨を通知するとともに、その理由を説明している | 1. 個人情報開示等請求に対するご通知
 |
| **J.8.8.2　第三者提供に係る記録の作成など**①医療連携を含む直接的な診療以外の目的で個人データを第三者に提供した場合、記録を作成、保管している | 個人情報保護規程第35条（診療以外の目的では）提供していない |
| ②記録の作成を要してしていないのは、J.8.8.2のａ)～ｊ)のいずれかに該当する場合に限定している | 個人情報保護規程第35条 |
| ③J.8.8.2のａ)～ｊ)を適用して記録を作成、保管しない場合は、定めた手順(J.2.4)に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報取扱申請書 |
| ④個人データを第三者に提供したことに関する記録を作成した場合、当該記録を必要な期間保管している | （診療以外の目的では）提供していない |
| ⑤個人データを提供したときに、提供先が実施する第三者提供を受ける際の確認等に対し、適切に応じること | （診療以外の目的では）提供していない |
| **J.8.8.3　第三者提供を受ける際の確認など**①医療連携を含む直接的な診療以外の目的で第三者から個人データの提供を受けるに際しては、必要な確認を行なっている | 個人情報保護規程第36条（診療以外の目的で）提供を受けていない |
| ②第三者から個人データの提供を受けるに際して確認を行ったときは、必要な記録を作成している | （診療以外の目的で）提供を受けていない |
| ③第三者から個人データの提供を受けるに際して確認を行った記録は、必要な期間保存している | （診療以外の目的で）提供を受けていない |
| ④確認の記録を作成していないのは、J.8.8.3 のa)～ｊ)のいずれかに該当する場合に限定している | 個人情報保護規程第36条 |
| ⑤J.8.8.3 のa)～ｊ)を適用して記録を作成、保管しない場合は、定めた手順(J.2.4)に則り事前に個人情報保護管理者等の承認を得ている（例：個人情報取扱申請書等により承認の記録が残ること） | 個人情報取扱申請書 |
| **J.8.8.4　個人関連情報の第三者提供の制限など**①個人関連情報を個人データとして提供を受ける事業者（提供先）は、以下の事項をあらかじめ本人に通知又は明示して同意を得ていること。 1)提供先の事業者の名称又は氏名 2)提供先の事業者の個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先 3)個人関連情報の提供を受けて個人データとして取得した後の利用目的 4)個人関連情報の項目 5)個人関連情報の取得方法 6)個人関連情報の取扱いに関する契約がある場合はその旨 | 個人関連情報は取り扱っていない |
| ②個人関連情報を提供する事業者（提供元）は以下の事項をあらかじめ本人に通知又は明示して同意を得ている1)提供元の事業者の名称又は氏名2)提供元の事業者の個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先3)個人関連情報の提供を受けて個人データとして取得した後の利用目的4)個人関連情報の項目5)提供する手段又は方法6)個人関連情報の提供を受けて個人データとして取得する者7)個人関連情報の取扱いに関する契約がある場合はその旨 | 個人関連情報の提供をしていない |
| ③第三者が個人関連情報を個人データとして取得することが想定される場合、当該個人関連情報を当該第三者に提供するに際しては、J.8.8のf)～l)のいずれかに該当する場合を除き、あらかじめ、J.8.8.4 のa)～b)に掲げる事項又はそれと同等以上の内容の事項について、確認を行っている | 個人関連情報の提供をしていない |
| ④J.8.8のf)～l)を適用する場合は、事前に個人情報保護管理者等の承認を得ている。（例：個人情報取扱申請書等により承認の記録が残ること) | 個人情報取扱申請書 |
| ⑤個人関連情報を外国にある第三者に提供する場合には、J.8.8.1 で定めるところによって、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講じている | 個人関連情報の提供をしていない |
| ⑥個人関連情報を提供する事業者（提供元）は、J.8.8.4 の c) ～f)の記録を作成、保管している | 個人関連情報の提供をしていない |
| ⑦個人関連情報を個人データとして提供を受ける事業者（提供先）は、J.8.8.4 のg)～j)の記録を作成、保管している | 個人関連情報の提供を受けていない |
| **J.8.9　匿名加工情報**1. 匿名加工情報の取扱いを行うか否かの方針が存在する
 | 個人情報保護規程第38条匿名加工情報取扱規程 |
| ②匿名加工情報を取り扱う場合、J.8.9 の a)～e)項に関する適切な取扱いを行う手順を内部規程として文書化している | 匿名加工情報取扱規程第4条～ |
| ③医療情報を匿名加工する場合は、個人情報保護委員会規則で定める基準に従って加工を行っている | 匿名加工情報取扱規程第4条～ |
| ④匿名加工情報の第三者提供を行っている場合、法律に基づいた公表を行っている | 匿名加工情報の取扱いについて（公表文） |
| ⑤匿名加工情報を医療機関等から取得し、利用する場合は提供元の医療機関等において匿名加工情報の取り扱いに関して法律に基づいた公表を行なっていることを確認している | ＨＰで確認している |
| ⑥作成した匿名加工情報を、本人を識別するために他の情報と照合することを禁止している（アクセス制限、アクセスログの取得および確認等） | 匿名加工情報取扱規程第10条 |
| ⑦医療機関等から個人情報の匿名加工を受託している事業者において、対応表を保持している場合は、事業者内においては個人情報として取り扱っている（J.3.1.1、J.3.1.3に関連） | 匿名加工情報取扱規程第11条 |
| 1. 匿名加工情報の作成を委託している場合においては、委託先の事業者が作成する匿名加工情報が、個人情報保護委員会規則で定める以下の5つの加工基準を満たすことを担保する旨を契約書等で明確にしていること

1）特定の個人を識別することができる記述等の削除2）個人識別符号の削除3）情報を相互に連結する符号の削除4）特異の記述等の削除5）個人情報データベース等の性質を踏まえたその他の措置 | 業務委託契約書（匿名加工情報） |
| ⑨匿名加工情報を作成し、第三者への提供を行っている場合は、第三者へ提供する都度、匿名加工情報が個人情報では無いこと（個人情報保護法に基づいて適切に加工されたものであること）の確認を行なっており、どのような根拠をもって“個人情報ではない”という評価をしたのかという記録（承認も含む）が残す手順を規定すること（少なくとも提供の都度、承認を残す旨の手順が規定され、運用されていること） | 匿名加工情報取扱規程第12条 |
| ⑧匿名加工情報の加工が不十分であったことにより意図せず特定の個人が識別可能となってしまった場合のその情報の取り扱いについての手順を規定すること | 匿名加工情報取扱規程第13条 |
| **J.8.10　仮名加工情報**①仮名加工情報を取り扱う場合には、仮名加工情報を取扱う方針が存在している | 個人情報保護規程第39条 |
| ②仮名加工情報を取り扱う場合には、適切な取扱いを行う手順を内部規程として文書化され、仮名加工情報を第三者に提供できるのは、ただし書きJ.8.10のｅ)～ｈ)に限定している | 個人情報保護規程第39条仮名加工情報取扱規程 |
| ③仮名加工情報を作成する場合には、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして、個人情報保護委員会規則で定める基準に従い、個人情報を加工している | 仮名加工情報取扱規程第4条～ |
| ④仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じている | 仮名加工情報取扱規程第10条 |
| ⑤仮名加工情報を利用する場合は、ａ)～ｄ)の事項を実施している | 仮名加工情報取扱規程第11条 |
| ⑥仮名加工情報である個人データを第三者に提供していない | 仮名加工情報取扱規程第12条で禁止と規定 |
| ⑦仮名加工情報の取扱いに関する苦情の適切かつ迅速な対応を行っている | 匿名加工情報取扱規程第13条 |
| ⑧仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去している | 匿名加工情報取扱規程第14条 |
| ⑨仮名加工情報の作成を委託している場合においては、委託先の事業者が作成する仮名加工情報が、個人情報保護委員会規則で定める加工基準を満たすことを担保する旨を契約書等で明確にしている | 業務委託契約書（仮名加工情報） |
| **J.9　適正管理** |  |
| **J.9.1　正確性の確保**1. 個人情報のバックアップを実施する手順が定められている
 | 個人情報保護規程第40条バックアップ一覧表 |
| ②個人情報の入力誤り防止に関するチェックの手順が定められている | 個人情報保護規程第41条作業工程表（健診業務） |
| ③取り違え防止に対する対策（特に、郵送先の誤りを防止する対策など）を定めている | 個人情報保護規程第42条作業工程表（健診業務） |
| ④定めた保管期限を過ぎた個人情報の消去・廃棄の状況とその記録を残す手順が定められている（特に、法令で保存義務のある記録（診療録、処方箋等）は分けて管理し、消去・廃棄の際には記録を残している） | 個人情報保護規程第第43条廃棄記録簿 |
| **J.9.2　安全管理措置****Ⅰ組織的安全管理**1. 外部サービスを利用する場合であって、当該サービス提供事業者が当該個人データを取り扱わないことになっているサービスを利用する場合は、適切な安全管理措置が図られるよう、あらかじめサービス内容の把握、評価等を行ったうえで利用していること
 | 委託先評価表 |
| ②来訪者・従業者の入退館（室）の管理方法（識別、制限機構、記録・確認など）を規定している | 安全管理規程第4条入退室管理簿（各部門） |
| ③個人情報の搬送・移動時（部門間を含む）の対策（紛失・盗難予防、授受の記録など）を規定している | 安全管理規程第5条各部門授受記録 |
| ④法人全体の情報システムのネットワーク図がある | 情報システム構成図 |
| ⑤スマートフォン・タブレット端末等を業務使用する際の安全管理策を定めている | 安全管理規程第6条 |
| ⑥スマートフォン・タブレット端末等の私物利用に関する制限措置を定めている | 安全管理規程第6条 |
| ⑦個人情報やノートPC等の持ち込み、持ち出しに関する規定がある | 安全管理規程第7条ノートＰＣ持出（持込）申請書 |
| ⑧情報システムのリモートメンテナンス時の安全管理措置が明確（回線種別、接続手順、作業報告等） | 安全管理規程第8条リモートメンテナンス実施報告書（委託先から受領） |
| ⑨システムの初期設定（Administrator等のIDやPWなど）を使用していない | 安全管理規程第9条 |
| ⑩従業者の採用・異動・退職等に伴う、ID・パスワードの管理手順（登録・変更・廃棄）がある | 安全管理規程第10条アクセス権限付与（削除）申請書 |
| ⑪ユーザのアカウントに、不必要な権限を付与しない（管理者権限等） | 安全管理規程第11条アクセス権限管理表 |
| **Ⅱ物理的安全管理**1. 個人情報の取扱・保管場所（サーバ室等）へのアクセス制御を実施している（入退制限と記録・確認）
 | 安全管理規程第4条入退室管理簿（各部門） |
| ②個人情報（記録媒体を含む）の保管場所は施錠している | 安全管理規程第12条 |
| ③外部記録媒体（USBメモリ等）の取扱いについて規定している（利用目的、保管方法、パスワード、暗号化、個体識別など） | 安全管理規程第13条ＵＳＢ管理簿 |
| ④機器・装置の物理的な保護について対策されている（盗難、破壊、破損、漏水、火災、停電、地震等） | 安全管理規程第14条 |
| ⑤クリアデスク、クリアスクリーンを実施 | 安全管理規程第15条 |
| ⑥個人情報毎（紙、電子媒体、情報機器）の廃棄手順（記録）が明確 | 安全管理規定第16条廃棄記録簿（各部門） |
| ⑦業務システム等とインターネットは物理的または論理的に分離、もしくはIP固定等による接続制限を実施している | 安全管理規程第17条システム毎に以下の措置を講じている・電子カルテ：物理的に分離している・健診システム：Ｌ３スイッチによる論理的分　　離・介護システム（クラウド）：ＩＰフィルタリングによる接続先の固定 |
| **Ⅲ技術的安全管理**1. ネットワークの安全対策は適切である（専用線、ＶＰＮ、ファイアウォール、ＩＤＳなど）
 | 安全管理規程第18条 |
| ②情報システムへのアクセスにおける利用者の識別と認証を行っており、パスワードは「医療情報システムの安全管理に関するガイドライン」を参照し、以下の様な措置を講じている1. 英数字、記号を混在させた13文字以上の推定困難な文字列
2. 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更させる（最長でも2ヶ月以内）
3. 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列ただし他の認証要素として必要な電子証明書等の使用にPIN等が望ましい設定されている場合には、この限りではない
 | 安全管理規程第19条 |
| ③職種毎に適切なアクセス制限を実施している | 安全管理規程第20条アクセス権限管理表 |
| ④アクセスログを取得し定期的に確認している | 安全管理規程第21条アクセスログ記録簿 |
| ⑤不正アクセスや脆弱性対策（ウィルス対策、セキュリティパッチ適用など）を実施している | 安全管理規程第22条 |
| ⑥無線LANを利用する場合の安全管理措置は適切であ　　る | 安全管理規程第23条 |
| ⑦IoT機器で医療情報を取り扱っている場合の安全管理措置を規定している | 安全管理規程第24条 |
| ⑧個人情報を取り扱うシステムとインターネットを併用する場合の措置は適切 | 安全管理規程第17条システム毎に以下の措置を講じている・電子カルテ：物理的に分離している・健診システム：Ｌ３スイッチによる論理的分　　離・介護システム（クラウド）：ＩＰフィルタリングによる接続先の固定 |
| ⑨SNSを利用して医療情報連携等の患者情報等の情報共有を行う場合は、リスク分析を実施したうえで対策を講じている | 安全管理規程第25条委託先→業務委託契約書を締結利用端末→ＩＰフィルタリングによる接続先の固定 |
| ⑩オープンなネットワーク接続を利用する場合は、リスク分析を実施したうえで安全管理措置を講じている（認定指針J.9.2.C.⑦（p.104）参照） | 安全管理規程第26条 |
| ⑪オンライン診療を実施する場合は、「オンライン診療の適切な実施に関する指針」の内容を確認するとともに、指針の内容に基づいた安全管理措置を講じること※認定指針付録「オンライン診療システム導入チェックリスト」を参考に、自組織及び委託先のシステム開発事業者において、オンライン診療システムが指針で求められている措置を講じられていることを確認することが望ましい | オンライン診療実施規程 |
| ⑫「民間PHR事業者による健診等情報の取扱いに関する基本的指針」の対象となるサービスを提供している事業者は、本指針の内容を確認するとともに、リスク分析を実施したうえで本指針基づいた安全管理措置を講じること※本指針に添付されている別紙「本指針に係るチェックシート」を参考に指針で求められている措置が講じられていることを確認することが望ましい | チェックシートで適合状況の監査を実施 |
| **J.9.3　従業者の監督**1. 従業者等との雇用契約時又は委託契約時に、個人情報の非開示契約を締結するように規定している（就業規則に守秘の規定があるなら不要）
 | 個人情報保護規程第第44条 |
| ②ＰＭＳに違反した際の措置が規定されている | 守秘誓約書、就業規則 |
| ③就業規則に含まれない者（実習生、ボランティア等）からも守秘誓約書を取得している | 個人情報保護規程第第44条 |
| ④就業規則等に離職後も守秘の条項が有効であるように規定している | 守秘誓約書を取得（実習生、ボランティア） |
| **J.9.4　委託先の監督**①委託先選定基準を定める手順及び選定基準の定期的見直しに関する手順が定められている | 委託先管理規程第4条 |
| ②具体的で運用可能な委託先選定基準があり、承認の手順が明確である | 委託先管理規程第4条委託先評価表 |
| ③委託先選定から契約書の締結までの具体的手順が明確である | 委託先管理規程第5条委託先評価表 |
| ④再委託を認める場合には、委託先と同等かそれ以上の安全管理措置を実施している事業者を選定している | 委託先管理規程第6条個人情報委託契約書 |
| ⑤ａ）～ｈ）の条項を含む委託契約書がある（ひな形等の様式を提出）a)委託者及び受託者の責任の明確化b)個人データの安全管理に関する事項c)再委託に関する事項　d)個人データの取扱状況に関する委託者への報告の内容及び頻度e)契約内容が遵守されていることを委託者が、定期的に、及び適宜に確認できる事項f)契約内容が遵守されなかった場合の措置g)事件・事故が発生した場合の報告連絡に関する事項h)契約終了後の措置 | 個人情報委託契約書 |
| ⑥業務委託（病院の窓口業務等）であっても、委託先の従業者にPMSに従った運用を求めている（契約書に明記するなど） | 委託先管理規程第7条個人情報委託契約書 |
| ⑦委託先と、特定した利用目的の範囲内で委託契約を締結している | 個人情報委託契約書 |
| ⑧契約終了時の個人情報の取り扱い（保管期限、返却及び消去に関する事項等）について契約書等で明確にしている | 個人情報委託契約書 |
| ⑨全ての委託先が漏れなく特定されていること（委託先一覧等） | 委託先一覧表 |
| ⑩委託契約書が当該個人データの保有期間にわたって保存されている | 委託先管理規程第8条個人情報委託契約書 |
| ⑪委託契約に基づき、委託先を適切に監督している | 個人情報委託契約書 |
| ⑫クラウドサービスを利用して医療情報の利用・保管をする場合は認定指針J.9.4.C.⑫の対応を実施している | 委託先管理規程第9条業務委託契約書（介護システム） |
| **J.10　個人情報に関する本人の権利** |  |
| **J.10.1　個人情報に関する権利**①保有個人データに関して、本人から開示等の請求等を受けた場合、J.10.4～J.10.7の規定によって、遅滞なくこれに応じている | 個人情報保護規程第45条個人情報開示等申請書個人情報開示等請求に対するご通知開示等申出対応記録 |
| ②従業者への対応手続きも明確である | 個人情報保護規程第46条 |
| ③J.8.8.2及びJ.8.8.3で作成した第三者提供記録に関して、本人から開示等の請求等を受けた場合、J.10.5の規定によって、遅滞なくこれに応じている | 個人情報開示等申請書個人情報開示等請求に対するご通知開示等申出対応記録 |
| ④保有個人データ 又は 第三者提供記録 に当たらないものとして、 J.10.1 に掲げるのa)～ d) のいずれかに限定している | 個人情報保護規程第47条 |
| ⑤J.10.1のa)～d)を適用する場合は、定めた手順(J.2.4)に則り事前に個人情報保護管理者等の承認を得ている（「個人情報取扱申請書」等により承認の記録が残る） | 個人情報取扱申請書 |
| **J.10.2　開示等の請求等に応じる手続** 1. 保有個人データ又は第三者提供記録の開示等の請求等に応じる手続が文書化され、J.10.2 のa)～d) の事項が含まれている
 | 個人情報保護規程第48条 |
| ②上記他、対応スケジュール、承認手順等を定めてい　る | 個人情報保護規程第48条 |
| ③保有個人データ又は第三者提供記録の開示等の請求等をすることができる代理人が妥当である－未成年者又は成年被後見人の法定代理人－開示等の求めをすることにつき本人が委任した代理人－患者が成人で判断能力に疑義がある場合は、現実に患者の世話をしている親族及びこれに準ずる者（診療情報の開示） | 個人情報保護規程第48条 |
| ④保有個人データの開示等の請求等に応じる手続きを定めるに当たっては、本人に過重な負担を課するものとならないように配慮している | 個人情報保護規程第48条 |
| ⑤本人からの請求などに応じる場合に、手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内において、その額を定めている | 個人情報保護規程第48条 |
| **J10.3　保有個人データ又は第三者提供記録に関する事項の周知など**①保有個人データ又は第三者提供記録に関し、J.10.3 のa)～g) の事項を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む） に置いている | 保有個人データについて（公表文）当該文書をHPで公表、もしくは本人からの要望に応じて紙媒体で交付 |
| ②当該文書を事業所内等での掲示やホームページでの公表、または本人からの要望があった場合は、遅滞なく回答できる手順がある | 個人情報保護規程第49条 |
| **J.10.4　保有個人データの利用目的の通知**①対応のための手順（求めに応じない場合を含む）が内部規程として文書化されている（様式、承認手順） | 個人情報保護規程第49条 |
| ②本人から，当該本人が識別される保有個人データについて，利用目的の通知を求められた場合，遅滞なくこれに応じている | 個人情報開示等申請書個人情報開示等請求に対するご通知 |
| ③本人から、当該本人が識別される保有個人データについて、利用目的の通知を求められた場合であって、利用目的の通知を必要としないのは以下の場合に限定していること・利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合・利用目的を本人に通知し、又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合・国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがある場合・J.10.3のc)によって当該本人が識別される保有個人データの利用目的が明らかな場合 | 個人情報保護規程第49条 |
| ④2項の各事由のいずれかに該当する場合で、利用目的の通知をしない場合は、定めた手順(J.2.4）に則り事前に個人情報保護管理者等の承認を得ている（「個人情報取扱申請書」等により承認の記録が残る） | 個人情報取扱申請書 |
| ⑤2項の各事由のいずれかに該当する場合、本人に遅滞なくその旨を通知するとともに、理由を説明していること | 個人情報開示等請求に対するご通知 |
| **J.10.5　保有個人データ又は第三者提供記録の開示**①対応のための具体的な手順（求めに応じない場合を含む）が内部規程として文書化されているされている（様式、承認手順） | 個人情報保護規程第50条 |
| ②本人から、当該本人が識別される保有個人データ又は第三者提供記録の開示の請求を受けた場合、法令によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、電磁的記録の提供も含めて当該本人が指定した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面 の交付による方法） によって開示している | 個人情報開示等申請書開示等申出対応記録 |
| ③本人から、当該本人が識別される保有個人データ又は第三者提供記録の開示の請求を受けた場合であって、全部又は一部の開示を必要としないのは以下の場合に限定しているa)本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合b)当該組織の業務の適正な実施に著しい支障を及ぼすおそれがある場合c)法令に違反する場合 | 個人情報保護規程第50条 |
| ④J.10.5 のa)～c)適用する場合は、定めた手順(J.2.4に則り事前に個人情報保護管理者等の承認を得ている（「個人情報取扱申請書」等により承認の記録が残る） | 個人情報取扱申請書 |
| ⑤J.10.5の1項の当該本人が指定した方法について、当該方法による開示が困難であるとして、書面での交付とした場合、もしくは、2項の各事由 のいずれかに該当する場合、本人に遅滞なくその旨を通知するとともに、理由を説明している | 個人情報開示等請求に対するご通知 |
| **J.10.6　保有個人データの訂正、追加又は削除** ①対応のための手順（求めに応じない場合を含む）が内部規程として文書化されている（様式、承認手順） | 個人情報保護規程第51条 |
| ②本人から、当該本人が識別される保有個人データの訂正等(訂正、追加又は削除)の請求を受けた場合、法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人データの訂正等を行っている | 個人情報開示等申請書開示等申出対応記録 |
| ③本人から保有個人データの訂正等の請求を受けて訂正等を行った場合は、その旨及びその内容を本人に遅滞なく通知している | 個人情報開示等請求に対するご通知開示等申出対応記録 |
| ④本人から保有個人データの訂正等の請求を受けたが応じなかった場合、その旨及びその理由を本人に遅滞なく通知している | 個人情報開示等請求に対するご通知開示等申出対応記録 |
| **J.10.7　保有個人データの利用又は提供の拒否権**1. 対応のための手順（求めに応じない場合を含む）が内部規程として文書化されている（様式、承認手順）
 | 個人情報保護規程第52条個人情報開示等申請書開示等申出対応記録個人情報開示等請求に対するご通知 |
| ②本人から当該本人が識別される保有個人データの利用停止等(利用の停止，消去又は第三者への提供の停止)の請求に応じている | 個人情報開示等申請書開示等申出対応記録 |
| ③本人からの当該本人が識別される保有個人データの利用停止等の請求に応じた場合，遅滞なくその旨を本人に通知している | 個人情報開示等請求に対するご通知開示等申出対応記録 |
| ④本人からの当該本人が識別される保有個人データの利用停止等の請求に応じなかった場合は以下の J.10.7 のa)～d)に該当する場合に限定（規定）し、本人に遅滞なくその旨を通知するとともに、理由を説明しているa)当該保有個人データの利用停止等に多額の費用を要する場合等の理由により、利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときb)本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合c)当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合d)法令に違反する場合 | 個人情報保護規程第52条個人情報開示等請求に対するご通知 |
| ⑤J.10.7 のa)～d)を適用する場合は、定めた手順(J.2.4に則り事前に個人情報保護管理者等の承認を得ている（「個人情報取扱申請書」等により承認の記録が残る） | 個人情報取扱申請書 |
| **J.11.1 苦情及び相談への対応**①個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順が内部規程として文書化されていること | 個人情報保護規程第53条 |
| ②本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行うための体制の整備を行っていること | 個人情報保護規程第53条個人情報保護体制図 |
| ③苦情及び相談への対応を実施していること | 個人情報苦情相談対応記録 |
| ④認定個人情報保護団体の対象事業者となっている場合は、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置いていること | HPで周知：https://aa.bb.ne.jp個人情報取り扱い同意書 |
| 99.　継続的改善事項1. 継続的改善を実施し記録を残している（前回審査にて継続的改善事項があった場合）
 | 【前回継続的改善事項】（１）業務システム（健診システム）へのアクセスには、個人別のID・パスワード等によるアクセス制限がないことから、ＯＳのID・パスワードで代用し管理しているこれでは、アクセスログの取得や、パスワードの管理にリスクが残る今後のシステムバージョンアップ等の機会に、適切なアクセス制限措置を実施すること【改善状況】システムバージョンアップにより個人別のID・パスワードが設定できるようになった（２） 業務システム（健診システム）の端末は、インターネットとの接続がないことからウィルスソフトがインストールされていないウィルスの感染経路はネットワークだけでないことから、ウィルス対策は重要であるリスク分析を実施し、必要なら何らかのウィルス対策を実施すること【改善状況】健診システムにウィルスソフトを導入（ウィルスサーバを設置して定期的更新を実施※ウィルスサーバは定期的に手動（媒体）で更新する） |

以上