「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４.１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４.１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４.１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. 事業の用に供している個人情報を適用対象とするよう定めている
2. 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
3. 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）
 | 1. 個人情報保護規程第1条
2. 個人情報保護規程第1条
3. 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　（本文4.1）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こと。 | 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　（本文4.2）利害関係者のニーズ及び期待の理解**①a)～b)を特定していること。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　（A.3.3.2）　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）
2. 特定・参照・維持の手順が明確（5W1Hの観点）
3. 見直し時期が明確である（少なくとも半年以内）
4. 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
5. 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 | 1. 個人情報保護規程第4条

法令等管理台帳1. 個人情報保護規程第4条
2. 個人情報保護規程第4条
3. 個人情報保護規程第4条
4. 法令等管理台帳でa)～t)を特定している
 |
| **J.1.4（本文4.3）　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こと。 | ―【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（本文4.4）　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こと。 | 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　（本文5.1）　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こと。 | 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（本文5.2.1、5.2.2、A.3.2.1、A.3.3.2）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）
2. ａ）～ｆ）の管理策が含まれている（特に目的外利用をしないことが明確）
3. 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
4. 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
 | 1. 個人情報保護方針
2. 個人情報保護方針
3. https;//aaa.ne.jp/privacy policy
4. 個人情報保護規程第７条
 |
| **J.2.3.1（本文5.3、A.3.3.4）　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こと。②個人情報保護体制に係る責任者、担当者（教育、苦情及び相談受付、監査員等）の役割・責任・権限を明確に定めている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④システム管理者を選任している | 1. 個人情報保護体制図
2. 個人情報保護規程第７条
3. 個人情報保護体制図
4. 個人情報保護体制図
 |
| **J.2.3.2（A.3.3.4）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トップマネジメントによって、役員クラスなどの組織外に対して責任を持つことができる者を内部から指名している
2. 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を規定している
3. 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、事業者のトップマネジメントに報告する旨を規定している。
4. 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を規定している。
5. 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
6. 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
 | 1. 個人情報保護規程第７条

個人情報保護体制図1. 個人情報保護規程第７条
2. 個人情報保護規程第７条
3. 個人情報保護規程第７条
4. 個人情報保護体制図
5. 院長を選任している
 |
| **J.2.4(A.3.1.1) 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(A.3.3.1) 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
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
3. 全ての個人情報の利用目的等が把握できる様式（管理台帳等）がある
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
1. 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が明確
2. 管理台帳の定期的な見直しに関する手順（時期を含む）が明確である
3. 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
4. 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
 | 1. 個人情報保護規程第8条

個人情報特定・リスク分析規定I1. 個人情報取扱申請書
2. 個人情報管理台帳
3. 個人情報管理台帳
4. 個人情報特定・リスク分析規定I
5. 個人情報特定・リスク分析規定I
6. 個人情報管理台帳
7. 個人情報管理台帳
 |
| **J.3.1.2(本文6.1.1) 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こと。 | 1. 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（6.1.2、A.3.3.3）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を規定している
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
3. リスクに応じた対策が明確である（対策はPMSに反映されていること）
4. 残留リスクを分析し、その後の対応が明確（運用の確認に反映させている）
5. 「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
6. リスクの定期的な見直しの手順（臨時を含む）が明確
 | 1. 個人情報保護規程第10条

個人情報特定・リスク分析規定Ⅱ1. 個人情報特定・リスク分析規定Ⅱ

リスク分析表1. 個人情報特定・リスク分析規定Ⅱ

リスク分析表1. リスク分析表
2. 個人情報特定・リスク分析規定Ⅱ
3. 個人情報特定・リスク分析規定Ⅱ
 |
| **J.3.2（本文6.2）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こと。 | 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（A.3.3.6）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を定めている（5W1Hの観点）
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)
3. 監査計画書の立案と承認及び維持管理の具体的手順を定めている（5W1Hの観点）
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)
5. 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必要な計画に、次の事項を含んでいること。

a)実施事項（例：教育名称・目的等/監査テーマ・項目等b)必要な資源（例：教育テキスト/監査チェックリスト等）c)責任者（例：教育責任者・実施者/監査責任者・監査人）d)達成期限（例：教育実施日/監査スケジュール）e)結果の評価方法（例：理解度テストの評価等。監査：トップマネジメントへの報告・改善指示等） | 1. 個人情報保護規程第12条

PMS教育規定第4条1. PMS教育年間計画書

PMS教育部門計画書1. 個人情報保護規程第11条

PMS監査規定第4条1. PMS監査年間計画書

PMS監査部門計画書1. PMS教育部門計画書

PMS監査部門計画書 |
| **J.4　支援** |  |
| **J.4.1（本文7.1）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こと。 | 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（本文7.2）力量**①a)～d)を行うこと。 | 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（本文7.3、A.3.4.5）　認識**1. J.3.3のa)教育実施計画に基づき、少なくとも年１回ａ）～d）の内容を定期的に教育することが明確
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）
3. 対象者全員に教育を実施したことの記録を残す手順がある
4. 受講者の理解度を確認する手順が明確
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
6. 教育研修用の教材（テキスト）を提出
7. 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
 | 1. 個人情報保護規程第15条

PMS教育規定第1条1. PMS教育規定第2条
2. PMS教育規定第5条

教育出欠名簿1. PMS教育規定第5条
2. PMS教育規定第6条

教育出欠名簿1. 20××年度教育テキスト
2. 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（本文7.4）　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こと。 | 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（A.3.3.7）　緊急事態への準備**1. 影響度に応じたレベル分けをして対応を定めている
2. 外部への報告先が具体的である（名称、窓口、電話番号など）
3. 緊急事態としての事故の定義、法により対象となる事象と個人データの定義、関係者への報告･連絡の手順が法令等と整合するよう内部規程として文書化されていること。
4. ③をふまえたうえで、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）監査を実施し確認1. 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
 | 1. 個人情報保護規程第16条

緊急事態対応規定第4条1. 緊急事態対応規定第5条

緊急事態報告先一覧1. 緊急事態対応規定第6条
2. 緊急事態対応規定第6条
3. 緊急事態対応報告書
 |
| **J.4.5.1（本文7.5.1、A.3.5.1）　文書化した情報**①PMS文書化した情報の範囲（様式、記録も含める）が明確であり、最低限、a)～f)が含まれている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。） | ①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、各下位規定・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（本文7.5.3）　文書化した情報の管理**①文書化した情報は、次の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 | 1. 個人情報保護規程第18条
2. 社内イントラで参照
3. アクセス制限（外部アクセス不可）
4. 社内イントラで参照
5. 社内イントラで参照
6. 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. PMS文書管理台帳
 |
| **J.4.5.3（本文7.5.2、A.3.5.2）　文書化した情報（記録を除く）の管理**①文書化した情報の管理について、少なくともa)～d)を含む、具体的な管理ルール（発行、改訂、保管、破棄等）を定めている②文書化した情報(記録を除く。)の管理を実施している | 1. 個人情報保護規程第18条
2. PMS文書管理台帳
 |
| **J.4.5.4（A.3.3.5）　内部規程**1. ａ）～ｏ）の管理策に対応する内部規定（手順書レベル）が定められている
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
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
 | 1. 個人情報保護規程第19条
2. PMS文書管理台帳
3. 個人情報保護規程第19条
 |
| **J.4.5.5（A.3.5.3）文書化した情報のうち、記録の管理**1. 記録の管理ルール（更新、保管、破棄等）が明確である
2. a)～l)の事項を含む必要な記録を作成している
 | 1. 個人情報保護規程第20条
2. PMS記録管理台帳
 |
| **J.5　運用** |  |
| **J.5.1（本文8.1-8.3、A.3.4.1）　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。
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。
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。
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。
5. ②～⑤の記録を保持している。
 | 1. 個人情報保護規程第21条

個人情報保護規程他、各規定1. 各PMS運用記録
2. 各PMS運用記録
3. 委託先一覧表、委託先評価表
4. 各PMS運用記録
 |
| **J.6　パフォーマンス評価** |  |
| **J.6.1（本文9.1、A.3.7.1）　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こと。
2. 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に反映し、定期的に実施状況を確認する手順が規定されている
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)の事項を決定すること。
4. 運用の確認のためのチェックリストがある
5. 少なくとも以下の確認した記録を残す規定がある
6. 最終退出時の社内点検（施錠確認等）
7. 入退館（室）の記録の定期的な確認
8. アクセスログの定期的な確認
9. 運用の確認を実施している
10. 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
11. 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
12. 監視及び測定の結果の証拠として、文書化した情報を保持している。
 | 1. 個人情報保護規程第22条１項
2. 個人情報保護規程第22条2項
3. PMS運用チェックリスト
4. PMS運用チェックリスト
5. 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
6. 是正処置記録簿
7. 個人情報保護規程第22条3項
8. 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
9. 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（本文9.2、A.3.7.2）　内部監査**1. 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規定されている
2. 個人情報保護監査責任者は、必要に応じ適切な監査員を選任し、監査計画書に従い、個人情報を取り扱う全部門に対し定期的（最低年１回、及び必要に応じて適宜）に監査を行っている。
3. 監査人は、自ら所属する部門を監査しないように規定されている
4. 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うこと。
5. 全部門の監査が実施されている
6. 明らかになった不適合については不適合及び是正処置（J.7.1）により実施することが明確
7. 内部監査の実施にあたっては、事前に監査テーマに則ったチェックリスト等を作成し、漏れなく確認している
8. 内部監査の実施にあたっては、内部規程と本認定指針との適合状況を監査している
9. 内部監査の実施にあたっては、運用状況の監査を実施している
 | 1. 個人情報保護規程第23条

PMS内部監査規定第1条～5条1. 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

PMS内部監査規定第6条1. PMS内部監査規定第7条
2. 内部監査報告書
3. 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
4. PMS内部監査規定第8条
5. 内部監査チェックリスト
6. 内部監査チェックリスト（適合性監査）
7. 内部監査チェックリスト（運用監査）
 |
| **J.6.3（本文9.3、A.3.7.3）　マネジメントレビュー**1. マネジメントレビューのインプットとして、監査報告だけでなく、a)～ｆ)及び事故報告等を含めて規定している
2. マネジメントレビューを実施するにあたり、ａ）～ｇ）の事項がインプットされている
3. 具体的な手順・期間（年１回及び必要に応じて適宜）を明確にして、マネジメントレビューを実施している
4. 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）
 | 1. 個人情報保護規程第24条
2. マネジメントレビュー実施記録
3. 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1. マネジメントレビュー実施記録
 |
| **J.7 改善** |  |
| **J.7.1（本文10.1、A.3.8）**1. 発見された不適合について、この管理策により是正処置を実施するという関係が明確
2. 実施のための手順にはａ）～ｅ）の内容が含まれている。また、以下の点にも留意していること
3. 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
4. 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
5. 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
6. 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）

③是正処置の立案にあたっては、発見された不適合が他の所でも発生しないようにするための措置を検討している | 1. 個人情報保護規程第25条
2. 個人情報保護規程第25条

是正処置実施記録1. 是正処置実施記録
 |
| **J.7.2（本文10.2、A.3.8） 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こと | ①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（A.3.4.2.1） 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）
2. 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）
 | 1. 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（当法人の利用目的について）、各同意書1. 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（当社の利用目的について）、各同意書 |
| **J.8.2（A.3.4.2.2）　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）
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
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
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
 | 1. 個人情報保護規程第28条
2. 個人情報保護規程第28条
3. 個人情報保護規程第28条
4. 個人情報保護規程第28条
 |
| **J.8.3（A.3.4.2.3）　要配慮個人情報**1. 保健医療福祉分野では、要配慮個人情報を主として取り扱うという観点から、個人情報の取得・利用・提供に際しては、あらかじめ書面による本人の同意を得ることが前提となる。
2. 要配慮個人情報を取得・利用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)-ｉ)の場合に限定している
3. 要配慮個人情報を提供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)-d)項又は、j)-l)項の場合に限定している
4. 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）
 | 1. 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）1. 個人情報保護規程第29条
2. 個人情報保護規程第29条
3. 個人情報取扱申請書（実績無し）
 |
| **J.8.4(A.3.4.2.4) 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
2. 利用目的を通知・公表するための文書がある
3. 本人への利用目的の通知又は公表を要しないのは、以下のただし書きa)～d)の場合に限定していること。

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組織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1. ただし書きを適用する場合は、定めた手順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を残している）
2. 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が明確
 | 1. 個人情報保護規程第30条
2. 利用目的公表文書（当法人の利用目的について）
3. 個人情報保護規程第30条
4. 個人情報取扱申請書（実績無し）
5. 個人情報保護規程第30条
 |
| **J.8.5(A.3.4.2.5) 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）
2. 取得場面毎に同意に用いる様式を整備している
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）
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
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
6. 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
1. ただし書きを適用する場合は、定めた手順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を残している）
2. 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
3. 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
4. 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
 | 1. 個人情報保護規程第30条
2. 各同意書

・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）1. 個人情報同意書（診療）
2. 個人情報保護規程第30条

個人情報同意書（採用応募時）（採用時）1. 個人情報保護規程第30条

Webフォーム（お問合せ等）1. 個人情報保護規程第30条
2. 個人情報取扱申請書
3. 個人情報保護規程第30条
4. 個人情報保護規程第30条
5. 個人情報保護規程第30条

個人情報同意書（健診） |
| **J.8.6(A.3.4.2.6)　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）がある。事例がないなら、その旨を明確にし、禁止している
2. 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方法によって個人情報の利用を行わない旨が文書化されていること。
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こと。
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
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.8.6のただし書きa)～f)のいずれかに該当する場合に限定している。
6. ただし書きを適用する場合は、定めた手順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を残している）
7. 学会発表等への利用について規定している
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。
 | 1. 個人情報保護規程第31条
2. 個人情報保護規程第31条
3. 利用していない
4. 個人情報保護規程第31条
5. 個人情報保護規程第31条
6. 個人情報取扱申請書
7. 個人情報保護規程第31条
8. 個人情報同意書
 |
| **J.8.7(A.3.4.2.7)　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）がある。事例がないなら、その旨を明確にし、禁止している
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こと。
3. 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 のただし書きa)～f)に限定していること。
4. ただし書きを適用する場合は、定めた手順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を残している）
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
 | 1. 個人情報保護規程第32条
2. 個人情報同意書
3. 個人情報保護規程第31条
4. 個人情報取扱申請書
5. 個人情報同意書（健診）
 |
| **J.8.8(A.3.4.2.8)　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）がある。
2. 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 のただし書きa)～g)に限定していること。
3. ただし書きを適用する場合は、定めた手順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を残している）
4. 2 項b)の適用にあたっては以下の1)～3)の個人情報及び個人データを除いていること。
5. 要配慮個人情報
6. 偽りその他不正の手段により取得された個人データ
7. 個人情報保護法二十七条第二項、又は J.8.8 の 2 項 b)により提供された個人データ（提供されたデータに対して、その全部又は一部を複製し、又は加工したものを含む）
8. 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）
9. 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）
10. 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
11. 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
12. 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。
13. 共同利用を行なっている場合、共同利用について共同利用者間で、以下の項目について契約等で定めている
* 共同して利用すること
* 共同して利用される個人情報の項目
* 共同して利用する者の範囲
* 共同して利用する者の利用目的
* 共同して利用する個人情報の管理について責任を有する者の氏名又は名称
* 取得方法
 | 1. 個人情報保護規程第33条
2. 個人情報保護規程第33条
3. 個人情報取扱申請書
4. 個人情報保護規程第33条
5. 個人情報保護規程第33条
6. 個人情報保護規程第33条
7. 個人情報同意書（健診）
8. 個人情報保護規程第33条
9. 個人情報同意書
10. 共同利用は実施していない
 |
| **J.8.8.1(A.3.4.2.8.1)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を規定していること。
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。
3. J.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.8.3のa) ～d) 、又は、J.8.3のj)～l)に限定していること。
4. ただし書きを適用する場合は、定めた手順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を残している）
5. 法令等の定めるところによって、 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こと。
6. 1項の 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、法令等の定めるところによって、ｊ）～l）の事項について、必要な措置を講じていること。
7. 3項のl) 項で、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こと。
 | 1. 個人情報保護規程第34条
2. 提供していない
3. 個人情報保護規程第34条
4. 個人情報取扱申請書
5. 外国への第三者へは提供していない
6. 外国への第三者へは提供していない
7. 外国への第三者へは提供していない
 |
| **J.8.8.2(A.3.4.2.8.2)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、保管していること。②記録には以下の様な事項を記載すること○本人同意を得ている旨○第三者の氏名又は名称その他の当該第三者を特定できる事項○個人データによって識別される本人の氏名その他の当該本人を特定できる事項○個人データの項目③記録を作成していないのは、J.8.8.2のただし書きａ)～ｊ)のいずれかに該当する場合に限定していること。④ただし書き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）⑤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すること。⑥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。 | 1. 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1. （診療以外の目的では）提供していない
2. 個人情報保護規程第35条
3. 個人情報取扱申請書
4. （診療以外の目的では）提供していない
5. （診療以外の目的では）提供していない
 |
| **J.8.8.3(A.3.4.2.8.3)　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、確認を行った記録を作成し、保管していること。②確認を行なった記録には以下の様な事項を記載すること○本人の同意を得ている旨〇第三者の氏名又は名称、法人である場合は代表者名○個人データの取得の経緯○個人データによって識別される本人の氏名その他の当該本人を特定できる事項〇個人データの項目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、必要な期間保存すること。④確認の記録を作成していないのは、J.8.8.3 のただし書きa)～j)のいずれかに該当する場合に限定していること。⑤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） | 1. 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1. （診療以外の目的で）提供を受けていない
2. （診療以外の目的で）提供を受けていない
3. 個人情報保護規程第36条
4. 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個人関連情報を取り扱う場合には、法令等の定めるところによって、適切な取扱いを行う手順を内部規程として文書化され、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に、法令等の定めるところによって、確認を行うことを要しないのは、J.8.3のａ)～ｄ)、又は、ｊ)～ｌ)のいずれかに該当する場合に限定していること。②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、あらかじめ、ａ)～ｂ)の事項又はそれと同等以上の内容の事項について、法令等の定めるところによって、確認を行っていること。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、確認を要しないのは、J.8.3のただし書きａ)～ｄ)、又は、ｊ)～ｌ)のいずれかに該当する場合に限定していること。④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）⑤個人関連情報を外国にある第三者に提供した場合には、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ること。⑥法令等の定めるところによって、ｃ)～ｆ）事項について、確認の記録を作成、保管すること。⑦法令等の定めるところによって、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、g)～j)の記録を作成、保管していること。 | 1. 個人情報保護規程第37条
2. 個人情報保護規程第37条
3. 個人情報保護規程第37条
4. 個人情報取扱申請書
5. 外国への第三者へは提供していない
6. 個人関連情報は取り扱っていない
7. 個人関連情報は取り扱っていない
 |
| **J.8.9（A.3.4.2.9）　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こと。
2. 匿名加工情報を取り扱う場合、匿名加工情報取り扱いの手順を内部規程として規定している
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
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
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
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）
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）
8. 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1. 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）
2. 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。
 | 1. 個人情報保護規程第38条

匿名加工情報取扱規程1. 匿名加工情報取扱規程第4条～
2. 匿名加工情報取扱規程第4条～
3. 匿名加工情報の取扱いについて（公表文）
4. ＨＰで確認している
5. 匿名加工情報取扱規程第10条
6. 匿名加工情報取扱規程第11条
7. 業務委託契約書（匿名加工情報）
8. 匿名加工情報取扱規程第12条
9. 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、法令等の定めるところによって、適切な取扱いを行う手順を内部規程として規定され、仮名加工情報を第三者に提供できるのは、ただし書きｅ)～ｈ)に限定していること。②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こと。③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こと。④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こと。⑤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こと。⑥仮名加工情報を提供する場合には、 J.8.10のｅ)～ｈ)のいずれかに該当する場合に限定していること。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こと。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こと。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こと | 1. 個人情報保護規程第39条

仮名加工情報取扱規程1. 仮名加工情報取扱規程第4条～
2. 仮名加工情報取扱規程第10条
3. 仮名加工情報取扱規程第11条
4. 仮名加工情報取扱規程第12条で禁止と規定
5. 匿名加工情報取扱規程第13条
6. 匿名加工情報取扱規程第14条
7. 匿名加工情報取扱規程第15条
8. 業務委託契約書（仮名加工情報）
 |
| **J.9（A.3.4.3）　適正管理** |  |
| **J.9.1（A.3.4.3.1）　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
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
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
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）
 | 1. 個人情報保護規程第40条

バックアップ一覧表1. 個人情報保護規程第41条

作業工程表（健診業務）1. 個人情報保護規程第42条
2. 個人情報保護規程第第43条
 |
| **J.9.2（A.3.4.3.2）　安全管理措置****Ⅰ組織的安全管理**1. 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
2. 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
3. 法人全体の情報システムのネットワーク図がある
4. 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
5. 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
6. 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
7. 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（ISDN回線によるダイアルアップPtoP接続など）
8. 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
9. 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
10. 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）
 | 1. 安全管理規定第4条

入退室管理簿（各部門）1. 安全管理規定第5条

各部門授受記録1. 情報システム構成図
2. 安全管理規定第6条
3. 安全管理規定第6条
4. 安全管理規定第7条

ノートＰＣ持出（持込）申請書1. 安全管理規定第8条
2. 安全管理規定第9条
3. 安全管理規定第10条

アクセス権限付与（削除）申請書1. 安全管理規定第11条
 |
| **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）
2. 個人情報（記録媒体を含む）の保管場所は施錠している
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）
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）
5. クリアデスク、クリアスクリーンを実施
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
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している
 | 1. 安全管理規定第4条

入退室管理簿（各部門）1. 安全管理規定第12条
2. 安全管理規定第13条

ＵＳＢ管理簿1. 安全管理規定第14条
2. 安全管理規定第15条
3. 安全管理規定第16条

廃棄記録簿（各部門）1. 安全管理規定第17条
 |
| **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）
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ること。
3. 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
4. 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）
5. 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。
6. 職種毎に適切なアクセス制限を実施している
7. アクセスログを取得し定期的に確認している
8. 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
9. 無線LANを利用する場合の安全管理措置は適切である
10. IoT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
11. 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
12. SNS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
13. 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
14. 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。
15. 「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。
 | 1. 安全管理規定第18条
2. 安全管理規定第19条
3. 安全管理規定第20条

　　アクセス権限管理表1. 安全管理規定第21条

アクセスログ記録簿1. 安全管理規定第22条
2. 安全管理規定第23条
3. 利用していない
4. 安全管理規定第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1. 安全管理規定第24条
2. 安全管理規定第25条
3. オンライン診療実施規程
4. 対象外
 |
| **J.9.3（A.3.4.3.3）　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）
2. 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
3. ＰＭＳに違反した際の措置が規定されている
4. 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
 | 1. 個人情報保護規程第第44条
2. 守秘誓約書、就業規則
3. 個人情報保護規程第第44条
4. 守秘誓約書を取得（実習生、ボランティア）
 |
| **J.9.4（A.3.4.3.4）　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。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）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）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こと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）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こと。⑪委託契約に基づき、委託先を適切に監督していること。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 | 1. 委託先管理規程第4条
2. 委託先管理規程第4条

委託先評価表1. 委託先管理規程第5条
2. 委託先管理規程第6条

個人情報委託契約書1. 個人情報委託契約書
2. 委託先管理規程第7条

個人情報委託契約書1. 個人情報委託契約書
2. 個人情報委託契約書
3. 委託先一覧表
4. 委託先管理規程第8条

個人情報委託契約書1. 個人情報委託契約書
2. 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（A.3.4.4）　個人情報に関する本人の権利** |  |
| **J.10.1（A.3.4.4.1）　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こと。②従業者への対応手続きも明確である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こと。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こと。⑤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（「個人情報取扱申請書」等により承認の記録が残る） | 1. 個人情報保護規程第45条
2. 個人情報保護規程第46条
3. 個人情報開示等申請書
4. 個人情報保護規程第47条
5. 個人情報開示等申請書
 |
| **J.10.2（A.3.4.4.2）　開示等の請求等に応じる手続** 1. 規格のa)～d)の事項について、応じる手順が、それぞれ規定されている（受付窓口、請求のための様式、本人確認、手数料の額等）
2. 上記他、対応スケジュール、承認手順等を定めている
3. 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）
1. 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
2. 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
 | 1. 個人情報保護規程第48条

個人情報開示等申請書1. 個人情報保護規程第48条
2. 個人情報保護規程第48条
3. 個人情報保護規程第48条
4. 個人情報保護規程第48条
5. 個人情報保護規程第48条
 |
| **J10.3（A.3.4.4.3）　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ついてa)～g)の事項を満たす文書がある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 | 1. 開示対象個人情報について（公表文）
2. 個人情報保護規程第49条
 |
| **J.10.4（A.3.4.4.4）　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）が明確（様式、承認手順）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こと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④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（「個人情報取扱申請書」等により承認の記録が残る）⑤ただし書きを適用する場合、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。 | 1. 個人情報保護規程第49条

個人情報開示等申請書1. 個人情報開示等申請書
2. 個人情報保護規程第49条
3. 個人情報開示等申請書
4. 個人情報開示等申請書
 |
| **J.10.5（A.3.4.4.5）　保有個人データ又は第三者提供記録の開示**①対応のための手順（求めに応じない場合を含む）が明確（様式、承認手順）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こと。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こと。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④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（「個人情報取扱申請書」等により承認の記録が残る）⑤1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こと。⑥法令上の義務について同意が得られない場合には、説明を行ったが拒否された旨を記録しておくことを規定している | 1. 個人情報保護規程第50条

個人情報開示等申請書1. 個人情報開示等申請書
2. 個人情報保護規程第50条
3. 個人情報開示等申請書
4. 個人情報開示等申請書
5. 個人情報保護規程第50条
6. 個人情報開示等申請書
 |
| **J.10.6（A.3.4.4.6）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）が明確（様式、承認手順）
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
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
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
 | 1. 個人情報保護規程第51条

個人情報開示等申請書1. 個人情報開示等申請書
2. 個人情報開示等申請書
3. 個人情報開示等申請書
 |
| **J.10.7（A.3.4.4.7）　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）が明確（様式、承認手順）
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
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
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 ａ)～ｃ)に該当する場合に限定していること。

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1. ただし書きを適用する場合は、定めた手順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を残している）
2. ただし書きを適用する場合、本人に遅滞なくその旨通知するとともに、理由を説明している
3. 法令上の義務について同意が得られない場合には、説明を行ったが拒否された旨を記録しておくことを規定している
 | 1. 個人情報保護規程第52条

個人情報開示等申請書1. 個人情報開示等申請書
2. 個人情報保護規程第52条
3. 個人情報保護規程第52条
4. 個人情報開示等申請書
5. 個人情報開示等申請書
6. 個人情報保護規程第52条
 |
| **J.11.1(A.3.6) 苦情及び相談への対応**①受付対応窓口が明確②対応のための具体的手順（本人に回答する内容の承認、受付・記録・報告）が明確③苦情及び相談への対応を実施していること④認定個人情報保護団体の対象事業者であるときは、当該団体の受付け先も明示している⑤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。 | 1. 個人情報保護規程第53条
2. 個人情報保護規程第53条

個人情報苦情相談対応記録1. https://aa.bb.ne.jp
2. 個人情報保護規程第53条
 |
| 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