保健医療福祉分野のプライバシーマーク認定指針第４版

Ｃ．最低限のガイドライン一覧

本資料の位置付け

- 本資料に示す項目は「保健医療福祉分野のプライバシーマーク認定指針第４版」において、最低限必要な審査項目となるＣ．最低限のガイドラインについて、JIS Q 15001:2017 の附属書Ａの項番毎に記述している。

また、本資料においては、審査項目毎に以下のような区分を設けている

- 文書審査：文書審査により規定の有無を確認
- 現地審査：現地審査により運用の記録を確認

※“現地審査”としている審査項目でも、事前に提出された運用記録等により確認する場合もある（例：個人情報管理台帳・教育監査記録等）

- 赤字：第４版で追加・変更した保健医療福祉分野独自の審査項目
- 青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）に合わせて追加・変更した審査項目

※青字で追加した審査項目で“現地審査”としている項目は、概ね従来の現地審査において運用確認していた事項を審査項目として明文化したものであるので特に更新審査においては、原則として新たな規定等を求めるものではない（ただし書きの適用など、事例がある場合は現地で運用状況を確認することとなる）

※本資料は印刷可能です

１　適用範囲（JIS 規格本文）

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	漏れなく個人情報保護マネジメントシステムが運用されるには、本マネジメントシステムに従った運用をする従業者の範囲も明確にしておくことが必要である。例えば、役員、職員だけでなく、パート、アルバイト、派遣職員、実習生、ボランティアなどの全従業者も含まれることを明確にする。	文書審査
②	事業の用に供している個人情報を適用対象とすることを明確にする。特に、従業者に関する個人情報や採用情報も対象となる点に留意する（A.3.3.1 に関連）。	文書審査

Ａ．３．１．１．一般

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	A.3.2 から A.3.8 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（個人情報管理者等による承認を得たことが確認できる記録を残していること）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．２．個人情報保護方針

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	個人情報保護方針（内部向け・外部向け）は、事業者の個人情報保護に関する取組みを内外に宣言する公式文書と位置づけられるものであることから、どのような理念で個人情報保護活動を行うのかを事業活動と関連させて明記するとともに、トップマネジメントは事業者の個人情報保護目的を説明できること（トップインタビューによる確認事項）。特に、個人情報保護法第３条（基本理念）では“個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ・・・”とされていることから、個人情報保護の理念とは、当該事業者が個人の人格尊重に基づいた個人情報保護に取り組む姿勢や基本的な考え方であることを認識し、個人情報保護法が求めている“人格尊重の理念”が個人情報保護方針に明確に反映されることが望ましい。	文書審査 現地審査 〈トップインタビューによる確認〉

②	個人情報保護方針（内部向け・外部向け）は、文書化した情報の範囲（A.3.5.1）に含まれていることから、文書化した情報の管理（A.3.5.2）に則った管理をしなければならない。当然ながら、公開している方針とマネジメントシステム文書の方針が一致していることが求められる。	文書審査
③	個人情報保護方針（内部向け・外部向け）は、単に内部の規程として従業者だけに周知徹底するだけではなく、書面等に文書化し、さらに、医療機関等を利用する患者等もその内容を知ることができるようにしなければならないことから、トップマネジメントは個人情報保護方針を、従業者（利害関係者も含む）や一般の人が入手可能な措置を講じておくこと（トップインタビューによる確認事項）。具体的には、外部向け個人情報の外部への公表手順としては、医療機関等の受付や診察室に掲示する、診療案内や診察券などに印刷する、診療時に書面を配布し説明する、ホームページ等で公開するトップページから直接リンクすることが望ましい）、などの方法が考えられる。また、内部向け個人情報保護方針の従業者が入手可能な措置としては、事務所内への掲示、イントラネットへの掲示などの方法が考えられる。	文書審査 〈公表手順〉 現地審査 〈トップインタビューによる確認〉
④	付録２１に医療機関における個人情報保護方針の例を示すとともに、以下に、管理策のａ）～ｆ）に対応する留意点を示す。 **ａ）事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること** 医療機関等においては、業務行為が、本来個人情報の取得そのものと考えることができる。従って、医療機関等においてマネジメントシステムを遵守するためには、個々の従業者が十分な自覚を持って適切な個人情報の取得、利用及び提供に努めなければならない。特に、現場においては、患者等の立場は弱く、また、健康上の問題から自分自身の個人情報保護に十分配慮することができない場面にも頻繁に遭遇するので、これらの点に関して適切な配慮が行われることが期待されている。また、当然のことながら、患者等から同意をいただいた目的以外に個人情報の利用を行わないこと及びそのための措置を講じることを明確にすることが必要である。 **ｂ）個人情報の取り扱いに関する法令、国が定める指針その他の規範を遵守すること** 医療機関等においては、患者等の情報は個人情報保護法、厚生労働省のガイドラインだけでなく、医師法及	文書審査

	び刑法 134 条などによっても保護されており、これらの規範を遵守するためにも、患者等の個人情報を保護するように努めなければならない。 **c）個人情報の漏えい、滅失又はき損の防止並び是正に関すること** 個人情報の漏えい、滅失、き損などに関して、物理的セキュリティ（建物や部屋の強度や出入りの制限など）、組織的セキュリティ（管理者やアクセス権限の設定など）、ネットワークセキュリティ（インターネットからのアクセス制限など）、コンピュータセキュリティ（ウイルスの混入防止など）をどのように確保し、防止に努めているのかを示す必要がある。 **d）苦情及び相談への対応に関すること** 個人情報に関する苦情及び相談への対応窓口を明示する。担当部署名、電話番号、e-mail アドレスなど具体的に示すこと。 **e）個人情報保護マネジメントシステムの継続的改善に関すること** 医療機関等のトップマネジメントは、その個人情報保護方針の中で、マネジメントシステムを実施し、管理する責任者を定め、どの程度の頻度で監査を定期的に行い、マネジメントシステムの遵守状況を評価し、計画を見直し、改善に努める旨を明確にしなければならない。特に、こうした努力を継続的に行う姿勢が重要である。 **f）トップマネジメントの氏名** 個人情報保護方針（内部向け・外部向け）を何時誰の責任で制定したのかを明確にしておくことが重要である。医療法人等で複数の医療機関がある場合などでは、法人全体の代表者である理事長と、医療機関の責任者である病院長の連名で明示することが望ましい。また、個人情報保護方針は、文書化した情報の範囲（A.3.5.1）に含まれており、文書化した情報の管理（A.3.5.2）の対象として、文書の発行及び改訂に関することを明示することが要求されているため、その制定年月日や改訂年月日を明らかにする必要がある。	

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．３．１　個人情報の特定

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	全ての個人情報の利用目的等が把握できるように管理台帳等を作成するなど、業務活動の中に個人情報を特定できる手順や仕組みを確立していること（定期的な見直しに関する手順を含む）。特に、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等への反映手順が明確であることが必要である。それには、個人情報の特定で使用する様式が規定されていることが求められる。	文書審査
②	台帳には少なくとも以下の項目が含まれていること。 －　個人情報の名称 －　件数（概数） －　個人情報の項目 －　利用目的 －　保管場所 －　保管方法 －　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（開示等の対象であるか否か）の識別 －　利用期限（特定した利用目的の範囲内で利用する期限） －　保管期限（個人情報を消去・廃棄するまでの期限）	現地審査
③	特定した個人情報が「保有個人データ」であるか否かの識別は、開示等への対応と関連しており、個人情報の適正管理の面から必要である。管理台帳等で「保有個人データ」（開示等の対象であるか否か）の識別が可能であること。	現地審査
④	全ての個人情報に保管期限（見直し時期という観点でも可）を定めていること。	現地審査
⑤	台帳の内容を少なくとも年一回、適宜に確認し、最新の状態で維持されていること。	現地審査

Ａ．３．３．２　法令、国が定める指針その他の規範

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	前記を例にその事業者で参照すべき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を特定し（名称、バージョン、発行日、発行者、URL 等）、参照し、維持する手順が定められているとともに、すべての従業者が参照可能な状態におくこと。	文書審査 現地審査 〈法令一覧〉
②	参照している国が定める指針その他の規範を定期的に見直し（少なくとも半年以内）、それらが改廃された場合、可及的速やかに個人情報保護マネジメントシステム文書や関連内規などにその改廃内容を必要に応じて反映する手順を定めていること。	文書審査
③	労働安全衛生法の一部を改正する法律により新たに設けられたストレスチェック制度の開始により、労働者に対してストレスチェックを実施する義務のある事業者および、事業者からの受託によりストレスチェック業務を実施している事業者（医療機関、健診機関、ストレスチェック事業者等）については、「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」において、衛生委員会の役割、ストレスチェックに用いる調査票、高ストレス者の選定方法、結果の通知方法と通知後の対応、面接指導結果に基づく就業上の措置に関する留意事項、集団ごとの集計・分析結果の活用方法、労働者に対する不利益な取扱いの防止、労働者の健康情報の保護などについて定められているため、該当する事業者は当該指針を特定し、参照・維持すること。	現地審査 〈法令一覧〉

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．３．３　リスクアセスメント及びリスク対策

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	A.3.3.1 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すること（リスクの定期的見直し手順を含む）。	文書審査
②	業務フロー等を活用し、A.3.3.1 によって特定した個人情報について、取得、移送、利用、保管、委託・提供、返却・廃棄までのライフサイクルに応じたリスクを分析し（取扱いの各局面におけるリスク）、対策を講じる具体的な手順を確	文書審査 現地審査

	立すること。	
③	リスクに応じた対策を明確にし、実施することとした対策はマネジメントシステム文書に反映すること。	文書審査 現地審査
④	新たな個人情報の取り扱いが発生した場合は当然として、取り扱いに変更があった際（取り扱う媒体の変更、ネットワーク構成や情報システムの変更、事務所の移転、個人情報の取り扱いに関する事故が発生した場合など）もリスクは変化することから、漏れなくリスク分析を実施する必要がある。常に台帳等によりリスクを把握し、取り扱いに変化が生じた場合においても「個人情報取扱申請書」等により特定し、リスク分析をするとともに、その結果を台帳等に反映するための具体的手順を規定すること。	文書審査 現地審査
⑤	リスク分析により実施することとした対策が適切に実施されているか、あるいは対策が妥当かどうかを定期的に確認することは重要である。特に残留リスクついては重点的に確認することが必要で、パフォーマンス評価（A.3.7）で用いるチェックリスト等に反映させ、定期的に確認する手順を確立すること。	文書審査
⑥	個人情報保護リスクの特定、分析及び講じた個人情報保護リスク対策を少なくとも年一回、適宜見直していること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．３．４　資源、役割、責任及び権限

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	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・権限を明確に規定すると共に、個人情報保護のための体制図等を整備し、従業者へ周知すること。	現地審査
②	個人情報保護管理者は、事業者の個人情報保護体制を公式に説明できる立場の者であること（原則として役員）。また、個人情報保護監査責任者は個人情報保護管理者を牽制する立場であることから、職制に大きな乖離がないこと。	現地審査
③	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こと。	文書審査
④	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	文書審査

	ていること。	
⑤	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こと。	文書審査
⑥	トップマネジメントが、個人情報保護のための人的資源を説明できること（トップインタビューによる確認事項）。	現地審査
⑦	個人情報保護監査責任者と個人情報保護管理者とは異なる者であること。	現地審査
⑧	電子カルテ等の情報システムを導入している場合は、システム管理者を内部から専任すること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．３．５　内部規程

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	ａ）～ｏ）に該当する、具体的な規程（手順書・様式を含む）を定めるとともに、必要に応じて容易に従業者が参照できる環境を整備すること。	文書審査 現地審査
②	内部規程の制定・改廃手続きについては、文書化した情報(記録を除く。)の管理（A.3.5.2）に基づく管理規程などを制定し、一定の手続きを経て規定・維持すること。	文書審査
③	医療情報を扱うシステムを導入している場合は、厚生労働省の定める運用管理規程（医療情報システムの安全管理に関するガイドライン参照）を制定していること（内部規程そのものが厚生労働省の求める運用管理規程を満足していることを明確にすることでも可）。医療情報システムには、電子カルテだけでなく、レセコン、健診システム、介護システム、検査センターの業務システム等、保健医療福祉分野の個人情報を取り扱う全てのシステムが含まれる。	文書審査

Ａ．３．３．６　計画策定

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	計画立案の時期、内容、承認方法、立案者など具体的な教育、監査計画の立案手順を定めること。	文書審査
②	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	現地審査

	b） 必要な資源 c） 責任者 d） 達成期限 e） 結果の評価方法	

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．３．７　緊急事態への準備

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	緊急事態の特定手順を策定するに当たっては、リスク分析（A.3.3.3）の結果を基に、リスクが顕在化した際の本人への影響度に応じたレベル分けをして対応を定めること。	文書審査
②	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医療機関等は（申請準備中、申請中を含む）、付与認定指定機関である（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すること。	文書審査
③	緊急事態への準備のため、以下のような観点で具体的手順を規定すること。 １）実態の把握と応急処置 ２）緊急連絡 ３）速やかに本人及び関係者に通知する ４）二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を遅滞なく公表する ５）関係機関（厚生労働省、自治体、認定個人情報保護団体等）に直ちに報告する ６）事故原因、本人への影響度、二次被害の有無等が明確になった時点で、本人への謝罪を行う ７）マネジメントシステムを見直し再発防止策を検討し実施する（対策の教育を含む） ８）監査を実施し、策定した再発防止策が問題なく機能しているか確認する	文書審査
④	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こと。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．１　運用手順

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	運用手順書や細則等は、あいまいさを作らないように″５Ｗ１Ｈ１Ａ１Ｒ″を明確にして作成すること。 who（誰が）、what（何を）、when（いつ、何時までに）、where（どこへ、どこで）、why（なぜ：理由・目的）、how（どのように：手段・方法）、Authorize（誰かの承認が必要なのかどうか）、Record（記録を残すのかどうか）。	文書審査

Ａ．３．４．２．１　利用目的の特定

NO	審査項目（C．最低限のガイドライン）	文書・現地
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こと（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、A.3.3.1 で特定した利用目的の範囲内である）。	現地審査
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こと（個人情報管理台帳等、通知又は公表の記録、本人に明示した書面（同意書）利用目的を明確にしている）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．２．２　適正な取得

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	定めた手順に従って、個人情報を適正に取得していること（A.3.3.5.f に該当する規程に基づき個人情報を取得していること。特に提供又は委託を受けて取得した場合に、提供元又は委託元が個人情報を適切に取り扱っていることを確認していること）。	文書審査 現地審査
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	文書審査

	当該患者等の保健医療福祉サービス遂行に必須のものに限定する。また、患者等以外から当該患者等に関する情報を取得する場合も必要性を十分検討した後に行い、可能であれば患者等に取得情報の内容と取得状況の説明を行うこと。	現地審査
③	意識障害、精神障害、乳幼児などで、説明による同意が困難な場合は、保健医療福祉サービス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。	文書審査 現地審査
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すること。	文書審査 現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

A．3．4．2．3　要配慮個人情報

NO	審査項目（C．最低限のガイドライン）	文書・現地
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。	現地審査
②	緊急時以外で、ただし書き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の取得、利用及び提供を実施する際は、事前に個人情報保護管理者等の承認を得ていること。（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

A．3．4．2．4　個人情報を取得した場合の措置

A．3．4．2．5　A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	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”の措置に準じたあらかじめ書面による本人の同意を得ることを原則とすることを明確にすること。	文書審査

②	個人情報を取得する場面（時期、対象）により同意を得るための手順や通知内容（利用目的等）は異なるはずである。ａ）～ｈ）の事項を本人に通知し、あらかじめ書面による本人の同意を得る手順を業務毎に規定する。例えば、職員（募集時、採用時等）、患者（入院、外来等）、利用者（健診時、介護サービスの開始時、入所時等）、看護学生（募集時、入学時等）など。	文書審査 現地審査
③	同意は、本人の署名、同意欄へのチェック、ウェブサイト上での同意ボタンの押下などの明示的な方法により、本人の意思が確認できることが必要となる。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」等の選択肢を設けること。	現地審査
④	ホームページで登録フォーム等を利用して個人情報を取得する場合は、安全対策（SSL 等により暗号化等）を講じると共に、本管理策（A.3.4.2.4）を満たす内容を通知し同意を得ること。	現地審査
⑤	意識障害、精神障害、乳幼児など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。	文書審査 現地審査
⑥	ただし書き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、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）（A.3.4.2.4 の管理策）。	現地審査
⑦	緊急時以外で、ただし書きを適用して同意なしに本人から直接書面により個人情報を取得する場合は、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）（A.3.4.2.5 の管理策）。	現地審査
⑧	以下に取得時、A.3.4.2.5 の管理策に則った患者等に明示する内容の留意点を示す。ｄ）、ｅ）については、事例がない場合でも省略せずに”・・・することはない”などと明示することが適切である。 ａ）医療機関等の名称とトップマネジメントの氏名。医療法人の場合は、理事長と病院長の連名が望ましい。 ｂ）医療機関等の個人情報保護管理者の氏名又は職名と所属及び連絡方法。苦情及び相談の連絡先が異なる場合にはそれも記載。 ｃ）A.3.4.2.1 で特定した利用目的のなかで、診療目的及び医療機関等の健全な管理のためのものを挙げる。さらにこれらの項目のうち、特定の目的に限って患者等が拒否した場合に利用しないものがある場合はその項目。また、以下の項目についても配慮することが望ましい。	文書審査 現地審査

	● 列挙した利用目的の中で利用時に個別に同意を得るか、同意が得られない場合はその目的で利用しないもの ● 列挙した利用目的の中で法律に基づくもの ● 列挙した利用目的の中で公益性が強く、初診時の了解を持って取得及び利用に同意したこととする項目。さらにこれらの項目のうち、特定の目的に限って患者等が拒否した場合に利用しないものがある場合はその項目 d）以下については診療の必要上、第三者に個人情報を提供する場合があることを明示する。 ● 患者等への医療の提供のため、他の医療機関等との連携を図ること ● 患者等への医療の提供のため、外部の医師等の意見・助言を求めること ● 患者等への医療の提供のため、他の医療機関等からの照会があった場合にこれに応じること ● 患者等への医療の提供に際して、家族等への病状の説明を行うこと e）外注検査のように、契約を締結した外部機関への情報の提供の有無と、委託業務の概要（事業者名である必要はない）。 f）開示・訂正等に応じる旨及び問い合わせ窓口。開示を求める方法と費用、及び開示を拒否する場合の理由。訂正を求められた場合に応じる条件。一括して削除を求められた場合に要求に応じない条件。（医師法、医療法、療養担当規則等で規定された保存期間など。） g）当該医療機関等が保健医療福祉サービスの遂行上（サービスの提供上）、必要と認め、患者等が情報の利用又は提供を拒否した場合には、診療（サービス）が十分行われない可能性があること。 h）「本人が容易に認識できない方法により個人情報を取得する」とは、例えばホームページによる cookie やウェブ･ビーコン情報の取得等が挙げられるが、その場合には、当該方法により個人情報を取得している旨及び取得する個人情報の内容を開示することが求められる。	
⑨	A.3.4.2.4 の管理策に則った利用目的を公表する手順を定めること（利用目的の公表文書は PMS 文書として文書管理台帳等で管理されていること）。	文書審査

⑩	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することが必要と考えられる。同意書の文面にその旨を明記するとともに、その際の対応手順を規定すること。	文書審査
⑪	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する場合、精密検査などの 2 次健診等の受診者の結果を紹介先の医療機関等から後日取得するケースがある。その場合においては、“健診の精度向上の為に紹介先の医療機関等と情報連携をする場合があります”等の文言を同意書などに明記するなどして、あらかじめ書面による本人の同意を得られる措置を講じること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．２．６ 利用に関する措置

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本措置を実施するための手順を規定すること。事例がないなら、恣意的運用を防ぐ意味からもその旨を明確にし、禁止すること。	文書審査
②	特定した利用目的の範囲外の利用に該当するかどうかの判断に迷う場合は、個人情報管理者等の承認を求めることを規定すること。	文書審査
③	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、A.3.4.2.5 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こと。	現地審査
④	緊急時以外で、ただし書き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、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．２．７　本人に連絡又は接触する場合の措置

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本措置を実施するための手順を規定すること。事例がないなら、恣意的運用を防ぐ意味からもその旨を明確にし、禁止すること。	文書審査
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、A.3.4.2.5 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。	現地審査
③	共同して利用する者から個人情報を取得する場合であって、共同して利用する者が A.3.4.2.7 の d)の措置を講じない場合、本人に対して、A.3.4.2.5 の a)～f)に示す事項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。	現地審査
④	保健医療情報等の要配慮個人情報の取り扱いを委託される場合は、できるかぎり本人からあらかじめ書面による本人の同意を得ること。	現地審査
⑤	緊急時以外で、ただし書き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、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．２．８　個人データの提供に関する措置

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本措置を実施するための手順を規定すること。	文書審査
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、A.3.4.2.5 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こと。	現地審査
③	緊急時以外で、ただし書き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、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査
④	意識障害、精神障害、乳幼児など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	文書審査

	者や保護者に提示し同意を得ること。ただし、親権者等による虐待が疑われる場合を除く。	現地審査
⑤	警察や検察等捜査機関からの照会や事情聴取への対応手順を定めること（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）。	文書審査 現地審査
⑥	健診業務の場合、法定健診項目と法定外健診項目で結果報告の手順を分けていること。健診結果（法定外健診項目）を事業者へ報告する場合は本人の個別の同意が前提となる（「雇用管理に関す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」第３の１参照）	文書審査 現地審査
⑦	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こと。 ○　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	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．２．８．１　外国にある第三者への提供の制限

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	外国にある第三者への提供を行う場合、あらかじめ本人の同意を得る手順を規定していること。	文書審査
②	外国にある第三者に個人データを提供する場合、外国にある第三者への提供を認める旨の本人の同意を得ていること（記録を残していること）。	現地審査
③	ただし書きを適用して本人の同意なしに個人情報を外国にある第三者に提供する場合は、事前に個人情報保護管理者等の承認を得ていること（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査

Ａ．３．４．２．８．２　第三者提供に係る記録の作成など

NO	審査項目（C．最低限のガイドライン）	文書・現地
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。	現地審査
②	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 ○　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	現地審査
③	ただし書きを適用して、記録を作成しない場合は、事前に個人情報保護管理者等の承認を得ていること。（例：個人情報取扱申請書等により承認の記録が残ること）。	現地審査

Ａ．３．４．２．８．３　第三者提供を受ける際の確認など

NO	審査項目（C．最低限のガイドライン）	文書・現地
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。	現地審査
②	確認を行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 ○　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 ○　個人データの項目	現地審査
③	ただし書きを適用して記録を作成、保管しない場合は、事前に個人情報保護管理者等の承認を得ていること。	現地審査

Ａ．３．４．２．９　匿名加工情報

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	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こと。	現地審査
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規定していること。	文書審査
③	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こと。	現地審査
④	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こと。	現地審査
⑤	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こと（アクセス制限、アクセスログの取得および確認等）。	現地審査
⑥	医療機関等から個人情報の匿名加工処理の委託を受け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うこと。	現地審査

Ａ．３．４．３．１　正確性の確保

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	正確性を損なうとどのようなリスクがあるのか、その発生可能性と発生した場合の重大性を評価し、予防対策及び発生時の対応策を定めること。A.3.3.3のリスク分析で実施することが適切である（分析の視点は正確性と安全性とは分けて行うこと）。	現地審査
②	正確性の確保に関する具体的措置は、個人情報の媒体の種類（紙媒体、電子媒体等）や、その取り扱いの方法により異なるので、媒体の種類や方法毎に適切な対策を規定し実施すること。以下に規定すべき最低限の留意点を示す。 ● 個人情報の保管期限を定める手順（3.3.3に関連） ● 個人情報のバックアップの手順（媒体の保管方法を含む） ● 個人情報の入力誤り防止に関するチェックの手順 ● 患者等の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）	文書審査 現地審査

	● 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（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すこと（付録２に保健医療分野の保存義務に関する法令等を示す）。	

Ａ．３．４．３．２　安全管理措置

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	安全性を損なうとどのようなリスクがあるか、その発生可能性と発生した場合の重大性を評価して対策を立てること。A.3.3.3のリスク分析で実施することが適切である（分析の視点は正確性と安全性とは分けて行うこと）。	現地審査
②	情報システムを利用する場合は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に則った運用管理規程を整備する必要がある（p22　C③参照）。また、医療情報の保管・処理を受託する事業者は、経済産業省の「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」、医療情報の処理をASP・SaaS・クラウド等で提供する事業者は、総務省の「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に準拠した体制を整備すること。	現地審査
③	情報システム等のメンテナンスを外注する際は、契約により安全性を担保すること（A.3.4.3.4に関連）。特に、外部からのリモートアクセスによるメンテナンス（リモートメンテ）を許可する場合は、その際の手順を規定すること（メンテナンス開始時や終了時の確認や記録、承認など）。	文書審査 現地審査
④	個人情報に対する安全性の確保のための具体的対策を規定すること。すなわち、誰がいつどのように行うのか具体的手順を定める（5W1H1A1Rの観点）。安全性の確保のための対策として下記のような留意点が上げられる。関係するものを選択し規定すること。	文書審査 現地審査
	Ⅰ　組織的安全管理 １）入退館（室）管理（来訪者・面会者への対応、記録・確認など） ２）個人情報の搬送・移動時の対策（紛失・盗難予防、授受の記録など） ３）法人全体の情報システム構成を俯瞰できるネットワーク図等の整備	

	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 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（業務システム端末等への接続制限など） ６）可搬型パソコン等の持ち込み／持ち出し時の安全管理 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 ８）ＯＳのディフォルトの設定を残さない（特権ユーザＩＤを使わない等） 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） １０）　ユーザのログインＩＤに、不必要な権限を付与しない（管理者権限等）	
	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（制限機構と記録・確認など） ２）個人情報の記録媒体の保管場所の安全管理（施錠など） ３）外部記憶媒体（DVD、USBメモリ等）の管理（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の対策（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 ６）個人情報毎（紙、電子媒体、情報機器、検体等）の廃棄手順（記録） ７）電子カルテ等の業務システムとインターネットの併用時の安全対策（原則として物理的に分離する）	
	Ⅲ　技術的安全管理 １）ネットワークの安全対策 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（ID、パスワード）。パスワードは、2ヶ月毎の変更（2要素認証を採用している場合を除く）、8文字以上の文字列が推奨される。 ３）職種毎の適切なアクセス制限 ４）アクセスログの取得と定期的な確認 ５）不正ソフトウェア対策（ファイル交換ソフト、ウイルス、パッチ当てなど） ６）無線LANを利用する場合の安全管理措置	

	7）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	
⑤	個人情報を取り扱うシステムとインターネットは、物理的分離を原則とすること。ただし、地域包括ケア等のために個人情報を取り扱うシステムとインターネットへ接続するシステムを併用する場合は、以下の対策を実施して個人情報を取り扱うシステムとインターネットへ接続するブラウザやアプリケーションが、同一端末で同時に利用できないようにすること。 １）リスク分析を実施し、リスクに対する対策の実施と残留リスクを把握 ２）ファイアウォール等による外部からの脅威への対策 ３）L3 スイッチ、デスクトップ仮想化技術等による内部からの漏出脅威への対策 ４）個人情報を取り扱うシステムが、クラウドサービス等のインターネットを経由したサービスを利用している場合は、IP フィルタリング等により接続先の限定を行なっている。 ５）不適切な運用の抑止及び追跡のためアクセスログの記録・解析（誰が、いつ、誰の情報に、どのようなアクセスをしたか等の詳細な情報を記録し、定期的な記録の確認を行う）をリアルタイム又は定期的に実施し、異常なアクセスがあったときは警告を発する機能等を付加する ６）論理的分離ポリシー及び機器のパラメータ設定を記録し、担当者が変わってもポリシーが維持されることを担保する	文書審査 現地審査
⑥	SNS を利用して医療情報連携等のために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、少なくとも以下の事項を踏まえること。 １）サービス利用者・家族に SNS を利用する旨、利用する SNS における情報の利用目的、対策事項等を説明し、同意を取得すること。 ２）利用している SNS は非公開型であること。 ３）SNS を利用する端末については接続先の限定、アクセス権限付与、パスワード運用、ウイルス対策、アクセスログの取得・確認等の安全管理措置を講じること ４）SNS を利用する要員に対する教育を実施すること。	文書審査 現地審査

	５）サービス提供事業者との間で SLA（Service Level Agreement）等が締結されサービス利用における責任分界点を明確にしていること。	
⑦	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、原則として以下のような措置を講じていること。 ○　IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンは TLS1.2 以上を利用し、TLS クライアント認証を実施している。 ○　SSL-VPN は偽サーバへの対策が不十分なものが多いため原則として使用しないこと。使用する（している）場合は、URL の書き換えを信頼できるドメインに限定する、VPN サーバの接続先を信頼できるドメインに限定する、URL の隠ぺい機能を無効にするなどの対策を講じていること。 ○　外部からのアクセス（自宅のパソコンやスマートフォン、タブレット端末等）を許可する場合、アクセスログの取得と確認、クライアント認証等によるアクセス制限などの安全管理措置を講じるとともに、運用管理規程を整備し、定期的に運用の点検と監査を実施すること。	文書審査 現地審査

Ａ．３．４．３．３　従業者の監督

NO	審査項目（Ｃ．最低限のガイドライン）	文書・現地
①	就業期間中はもとより離職後も含めた守秘義務を明記した誓約書等を取り交わすなど、雇用契約や就業規則において、従業者の個人情報保護に関する規程を整備し、徹底を図ること。従業者との守秘義務契約は、契約書（派遣職員等の場合）や就業規則に記載があれば個別に締結することは不要。	文書審査 現地審査
②	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すること。	現地審査
③	守秘義務契約及び個人情報保護マネジメントシステムに違反した際の措置を規定（就業規則の準用など）すること。	文書審査
④	ビデオ及びオンラインにより従業者のモニタリングを実施する場合に、その実施に関する事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて協議を行うよう規定すること。	文書審査

Ａ．３．４．３．４　委託先の監督

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	委託先選定基準を定める手順、及び選定基準が陳腐化しないための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こと。委託先選定基準は、具体的で運用可能なものであるとともに、承認手順が明確である必要がある。	文書審査
②	委託先選定基準により選定した委託先を承認する手順、及び承認した委託先との契約締結までの具体的手順を定め、ａ）～ｈ）の条項を含む契約書のひな形を準備し、契約内容に漏れがないようにすること。	文書審査
③	委託先を選定する基準は、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できるものでなければならない。	現地審査
④	個人に委託する場合であっても、委託先選定基準による選定が必要である。なお、優越的地位にある者が委託者の場合、委託先に不当な負担を課すことがあってはならない。	現地審査
⑤	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すること。	現地審査
⑥	医療機関等では窓口業務等を業務委託する例があるが、この場合は派遣業務と異なり医療機関等は業務委託された従業者への指揮命令権は持たない。しかし、個人情報の取扱いは医療機関等の従業者と変わりがないことから、業務委託であっても、本マネジメントシステムに従った運用を求めること（業務委託契約書に明記するなど）。	現地審査
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。	現地審査
⑧	契約終了後も、委託先に個人情報が残存することはリスクとなることから（提供と同等の状態となる恐れがある）、契約終了時の個人データの取り扱い（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すること。	現地審査
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、委託先の評価記録、委託契約書等で委託している全ての事業者を把握していること）。	現地審査
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。	現地審査
⑪	委託契約に基づき、委託先を適切に監督していること。	現地審査
⑫	クラウドサービスを利用して医療情報等の利用・保管等をする場合は、少なくとも以下の事項を踏まえること。 １）クラウドサービスを利用する医療機関等は自ら負うリスクを鑑みたうえで、クラウドサービス事業者との間で締	現地審査

	結する SLA（Service Level Agreement）等の内容を十分に検討しリスクの低減や回避を図ること。 ２）クラウド上に保管している患者情報等のデータが、法律や省令（e-文書法等）で保存義務があるデータである場合は、「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に基づき、所管官庁に対して法令に基づく資料を円滑に提出できるよう、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置していること。 ３）クラウド上に保管している患者情報等のデータが、法律や省令（e-文書法等）で保存義務が定められていないデータである場合は、事業継続を踏まえたリスク分析及びリスク対策を実施したうえで利用すること（別途バックアップを取得・保管するなど）。	

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．４．１　個人情報に関する権利

NO	審査項目（Ｃ．最低限のガイドライン）	文書・現地
①	個人情報に関する権利は、患者等の個人情報だけでなく従業者の個人情報も同様な対応が求められるため、従業者に対しても A.3.4.4.2～A.3.4.4.7 の管理策に対応した手続きを定めること。	文書審査
②	ただし書きを適用し、保有個人データとしない場合は、事前に個人情報保護管理者等の承認を得ていること。（例：「個人情報取扱申請書」等により承認の記録が残る）。	現地審査

Ａ．３．４．４．２　開示等の請求等に応じる手続

NO	審査項目（Ｃ．最低限のガイドライン）	文書・現地
①	開示等の求めに応じる手順を、具体的に規定すること（受付窓口、請求のための様式、本人確認、手数料の額、対応スケジュール等）。	文書審査
②	以下のような開示等の求めをすることができる代理人の範囲を明確にしておくこと。 －未成年者又は成年被後見人の法定代理人	文書審査

	ー開示等の求めをすることにつき本人が委任した代理人 ー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）	
③	従業者への対応手続きも規定すること。	文書審査
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こと。	現地審査
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こと。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．４．３　保有個人データに関する事項の周知など

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	保有個人データについて、ａ）～ｆ）の事項を院内や事業所内等へ掲示するか、あるいは患者等からの要望があった場合は遅滞なく回答できる手順を確保すること。	文書審査

Ａ．３．４．４．４　保有個人データの利用目的の通知

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。	文書審査
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。	現地審査
③	ただし書きを適用し、利用目的の通知を求められながら対応できない場合は、事前に個人情報保護管理者等の承認を得ていること。（例：「個人情報取扱申請書」等により承認の記録が残る）。	現地審査
④	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。	現地審査

Ａ．３．４．４．５　保有個人データの開示

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	開示のための具体的手順（様式等）を規定すること。	文書審査
②	ただし書きを適用し、保有個人データの開示をしない場合は、事前に個人情報保護管理者等の承認を得ていること。（例：「個人情報取扱申請書」等により承認の記録が残る）。	現地審査
③	保有個人データである診療情報の開示に当たっては、厚生労働省の「診療情報の提供等に関する指針」の内容にも配慮すること。	現地審査
④	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すること	文書審査
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。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．４．６　保有個人データの訂正、追加又は削除

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。	文書審査
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こと。	現地審査
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こと。	現地審査
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こと。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．４．４．７　保有個人データの利用又は提供の拒否権

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。	文書審査
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こと。	現地審査
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こと。	現地審査
④	ただし書きを適用し、利用又は提供の拒否を求められながら対応できない場合は、事前に個人情報保護管理者等の承認を得ていること。（例：「個人情報取扱申請書」等により承認の記録が残る）。	現地審査
⑤	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こと。	現地審査
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すること。	文書審査

Ａ．３．４．５　認識

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	事業者としての個人情報保護に対する理解度は従業者の認識レベルの最下層となることを認識し、全ての従業者にａ）～d）の内容を含む適切な教育を定期的（最低年１回）に実施する手順が規定されていること。教育対象には、雇用関係の有無にかかわらず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。	文書審査 現地審査
②	教育に際しては、個人毎に出欠を取り、欠席者にも漏れなく教育をすることが必要（欠席者のフォローアップ手順を定める）。また、教育対象を明確にし、従業者全員に教育を実施した記録を残すこと。	文書審査 現地審査
③	感想文やアンケート、小テストなどを実施することにより従業者の理解度を把握し、教育を受けたことを自覚させる仕組みを取り入れること（不合格者のフォローアップ手順を定める）。また、従業者の理解度等により、必要に応じて教育内容の見直しを図ること。	文書審査 現地審査

Ａ．３．５．１　文書化した情報の範囲

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	文書体系図等を作成し、個人情報保護マネジメントシステムとして管理すべき範囲が明確（様式、記録も含める）であること。	現地審査
②	マネジメントシステム文書を必要に応じて従業者が参照できる環境を整備すること。	現地審査

Ａ．３．５．２　文書化した情報(記録を除く。)の管理

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	文書の管理について、少なくとも a)～c)を含む、具体的な管理ルール（発行、改訂、保管、破棄等）を定めること。	文書審査
②	文書化した情報(記録を除く。)の管理を実施していること。	現地審査
③	各文書に目次や見出しラベルを付けるなど閲覧性を高める工夫をし、従業者が必要な文書を容易に参照することができるように努めること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．５．３　文書化した情報のうち記録の管理

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	記録の管理について具体的な管理ルール（作成、保管、破棄等）を定めること。	文書審査
②	a)～l)の事項を含む必要な記録を作成していること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．６　苦情及び相談への対応

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	苦情及び相談の窓口を明確にするとともに、受付担当者を任命しておくこと。	現地審査
②	本人に回答する内容の承認手順や、苦情及び相談の内容及び対応結果の記録手順を規定すること。	文書審査
③	苦情及び相談への対応を実施していること。	現地審査
④	認定個人情報保護団体の対象事業者であるときは、苦情受付時に当該団体の受付先も通知すること。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．７．１　運用の確認

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	リスク分析（A.3.3.3）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手順を定めること。	文書審査
②	少なくとも以下の事項の記録を残し定期的に確認する手順を確立すること。 ● 最終退出時（部門での業務終了時又は交代時など）の点検（施錠確認等） ● 入退館（室）の記録（最初に出社した人と最後に退社した人の記録） ● 個人情報を取り扱う情報システムのアクセスログの定期的確認	現地審査
③	運用の確認を実施していること。	現地審査
④	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こと。	現地審査
⑤	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の状況を報告する手順が規定され、報告していること。	文書審査 現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．７．２　内部監査

NO	審査項目（C．最低限のガイドライン）	文書・現地
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。	文書審査
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）に監査を行うこと。	現地審査
③	監査員は、原則として自己の所属する組織の監査をしてはならない（看護部を監査する場合は、看護部以外から監査員を選任するなど）。	現地審査
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。	現地審査
⑤	監査の実施に当たっては、事前に監査テーマに則ったチェックリスト等を作成し、漏れなく確認する手順を確立すること。	現地審査
⑥	チェックリスト等は、原本（各監査員が実際に使った手書きの用紙等）も実施記録として保管すること。	現地審査
⑦	内部監査の実施にあたっては、内部規程と JIS 及び本認定指針との適合状況を監査していること。	現地審査
⑧	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こと。	現地審査
⑨	トップマネジメントは、明らかになった不適合については、是正処置（A.3.8）により実施すること。	文書審査 現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．７．３　マネジメントレビュー

NO	審査項目（C．最低限のガイドライン）	文書・現地
①	見直しの根拠としてａ）～ｇ）を準備することを規定すること。	文書審査
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こと。	現地審査
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すること。	文書審査 現地審査

④	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こと（トップインタビューによる確認事項）。	現地審査
⑤	少なくともマネジメントレビューを年１回実施し（時期を明確にする）、その実施の記録（議事録等）を残すこと。	文書審査 現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

Ａ．３．８　是正処置

NO	審査項目（C．最低限のガイドライン）	文書・現地
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であること。	文書審査
②	実施のための手順にはａ）～ｅ）の内容が含まれているとともに、以下の点に留意していること。 • 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 • 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 • 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 • 個人情報保護監査責任者は、独立性の観点から改善案の立案・承認に関与しないことを原則とすること（有効性のレビューは除く）	文書審査 現地審査
③	医療機関等は、緊急事態への準備(A.3.3.7)、苦情及び相談への対応（A.3.6)、運用の確認(A.3.7.1)、監査(A.3.7.2)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・様式を整備すること。	文書審査 現地審査
④	是正処置の立案にあたっては、発見された不適合が他の部門等でも発生しないようにするための措置を検討していること。	現地審査
⑤	個人情報保護マネジメントシステムを継続的に改善していること（トップインタビューによる確認事項）。	現地審査

青字：プライバシーマーク付与適格性審査基準（JIPDEC 公表）

以上