ＰＭＫ－０１０

個人情報保護規程

第２．１版

発行日：2022年８月９日

承認日	作成日
2022年８月９日	2022年８月５日
承認者	作成者
中目　千之	渡邉　一夫

改版履歴

版数	発　行　日	改　訂　内　容
1.0	2005. 4. 1	初版発行
2.0	2021. 4. 1	第２版発行
2.1	2022. 8. 9	プライバシーマーク付与適格性審査の指摘事項に関する対応

目　次

1.　適用範囲

1.1 目的

この規程は、公益財団法人やまがた健康推進機構（以下、「健康推進機構」という。）が取り扱う個人情報の適切な利用と保護のため、日本工業規格 JIS Q15001：2017「個人情報保護マネジメントー要求事項」及び「個人情報の保護に関する法律」（以下、「個人情報保護法」という。）の要求事項に準拠した個人情報マネジメントシステムを確立し、実施、維持、かつ、改善を行うことを目的とする。

1.2 適用範囲

健康推進機構の個人情報保護マネジメントシステム（以下、「ＰＭＳ」という。）は、健康推進機構が事業の用に供して取り扱う全ての個人情報と、全ての従業者（評議員、理事、監事、医師、正規職員、嘱託職員（無期雇用を含む）、日々雇用職員、派遣社員、退職者）に対して適用する。

2. 用語及び定義

この規程で用いる主な用語及び定義は『個人情報保護マネジメントシステムー要求事項』(JIS Q 15001:2017)（以下、「この規格」という。）の用語及び定義に準じ、以下のとおりとする。

2.1　個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの。(他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。)

2.2　個人データ

個人情報のうち、個人情報を体系的に検索できるようにしたもの。

2.3　保有個人データ

個人データのうち、開示、訂正、消去等の権限を有し、6ヶ月以上保有するもの。

2.4　本人

個人情報によって識別される特定の個人。

2.5　事業者

事業を営む法人その他団体又は個人。

2.6　個人情報保護管理者

理事長によって組織内部に属する者の中から指名された者であって、個人情報保護マネジメントシステムの計画及び運用に関する責任及び権限をもつ者。(以下、「保護管理者」という。)

2.7　個人情報保護監査責任者

理事長によって組織内部に属する者の中から指名された者であって、公平かつ客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。(以下、「監査責任者」という。)

2.8　従業者

個人情報取扱事業者の組織内にあって直接間接に組織の指揮監督を受けて組織の業務に従事している者などをいい、雇用関係にある従業員（医師、正規職員、嘱託職員（無期雇用を含む）、日々雇用職員など）だけでなく、雇用関係にない従業者（評議員、理事、監事、派遣社員、退職者など）も含まれる。

2.9　個人情報保護リスク

個人情報の取扱いの各局面（個人情報の取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄に至る個人情報の取扱いの一連の流れ）における、個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人の権利利益の侵害など、好ましくない影響。

2.10　リスク

目的に対する不確かさへの影響。

2.11　残留リスク

リスク対応後に残っているリスク。

2.12　リスク対応

リスクを修正するプロセス。

2.13　脅威

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。

2.14　ぜい弱性

一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。

2.15　管理策

リスクを修正する対策。

2.16　緊急事態

個人情報保護リスクの脅威が顕在化した状態。

2.17　本人の同意

本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて承認する意思表示。本人が子ども又は事理を弁識する能力を欠く者の場合は、法定代理人等の同意も得なければならない。

2.18　個人情報保護

組織が、自らの事業の用に供する個人情報について、その有用性及び個人の権利利益に配慮しつつ、保護すること。

2.19　個人情報保護マネジメントシステム（Personal information protection management systems）

事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。（以下、「ＰＭＳ」という。）

2.20　不適合

JIS 規格『個人情報保護マネジメントシステム－要求事項』の要求事項を満たしていないこと。

A.3　管理目的及び管理策

A.3.1　一般

A.3.1.1　一般

この規程に規定する A.3.2 から A.3.8 は、理事長によって権限を与えられた者によって、健康推進機構が定めた手段に従って、承認するための手続きを各条項に定める。

A.3.2　個人情報保護方針

A.3.2.1　内部向け個人情報保護方針

(1) 理事長は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持する。

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。[特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、「目的外利用」という。）を行わないこと及びそのための措置を講じることを含む。]。

b）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遵守すること。

c）個人情報の漏えい、滅失又はき損の防止及び是正に関すること。

d）苦情及び相談への対応に関すること。

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。

f）理事長の氏名

(2) 理事長は、この方針を文書（電子的方式、磁気的方式など人の知覚によっては認識できない方法で作られる記録を含む。以下、同じ。）化し、従業者に周知させるとともに、利害関係者が入手可能な措置を講じる。

(3) 理事長は、「個人情報保護方針」をホームページで公表することにより利害関係者が入手可能な措置を講じる。また、従業者に周知させるために、社内イントラネットで閲覧可能な措置を講じるとともに、社内教育を行うものとする。

A.3.2.2　外部向け個人情報保護方針

(1) 理事長は、内部向け個人情報保護方針に加えて、次の事項を明記した、外部向け個人情報保護方針を定めるとともに、ホームページで公表することにより一般の人が入手可能な措置を講じる。

a）制定年月日及び最終改正年月日

b）外部向け個人情報保護方針の内容についての問い合わせ先

個人情報保護方針

公益財団法人やまがた健康推進機構（以下、“健康推進機構”という。）は、高度な情報通信社会の進展に伴い、個人情報の利用が著しく拡大していることに鑑み、事業の用に供する全ての個人情報を安全かつ正確に保護することが重要な社会的責任であること、また業務のなかで取扱う検（健）診・検査等の健康情報は、個人情報の中でも重要であることを深く認識し、厳正に取扱います。個人情報の有用性に配慮しつつ、個人の権利利益を適切・適正に保護・管理するために、役員及び職員が遵守すべき行動基準として本個人情報保護方針を定め、日本産業規格「個人情報保護マネジメントシステム - 要求事項」（JIS Q 15001）に準拠した個人情報保護マネジメントシステムを策定し遵守します。

１．健康推進機構は、事業遂行のために必要な範囲内で利用目的を明確に定め、適切に個人情報の取得、利用及び提供を行います。取得した個人情報は利用目的の範囲内でのみ利用し、目的外利用を行わないための措置を講じます。
２．健康推進機構は、取得した個人情報の取扱いの全部または一部を委託する場合には、十分な保護水準を満たした者を選定し、契約等により適切な措置を講じます。
３．健康推進機構は、すべての事業で取り扱う個人情報および職員等の個人情報に関して、個人情報保護に関する法令、国が定める指針及びその他の規範を遵守いたします。
４．健康推進機構は、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん、漏洩等のリスクに対して合理的な安全対策及び是正措置を講じます。
５．健康推進機構は、本人からの当該個人情報の利用目的の通知、開示、訂正、削除、利用停止等の要請及び苦情や相談に対して遅滞無く対応いたします。
６．健康推進機構は、個人情報保護マネジメントシステムを継続的に見直し改善いたします。

制定：2005 年 04 月 01 日
改定：2020 年 10 月 01 日
公益財団法人やまがた健康推進機構
理事長　中　目　　千　之

当機構の個人情報保護方針の内容や苦情、相談等の問合せ先
総務課総務係
電話：023-688-8333　　FAX：023-688-3734
e-Mail：jimukyoku@yamagata-yobou.jp

A.3.3　計画

A.3.3.1　個人情報の特定

(1) 健康推進機構は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持する。

1) 事業で取扱う個人情報、従業者の個人情報（以下、「インハウス情報」という。）、マネジメントシステムの運用において発生する記録類、業務の中で二次的に作成する管理資料、バックアップ情報などの棚卸を行い「個人情報管理台帳」に特定する。
2) 個人情報の特定は、個人情報を取扱う各部門の個人情報保護部門管理責任者（以下、「部門管理責任者」という。）が、毎年定期的に４月に行う。また、事業の変更、取扱う環境等の変化に伴い取り扱う個人情報に変更が生じた場合は随時、見直しを行う。
3) 各部門単位に特定した「個人情報管理台帳」は、保護管理者の承認を得る。
4) 「個人情報管理台帳」には、管理項目として以下の項目を含める。
   - 個人情報名称
   - 個人情報の項目
   - 利用目的
   - 件数
   - 情報形態
   - 要配慮区分
   - 取得（取得元、取得区分、取得媒体）
   - 利用（利用可能者、利用期限）
   - 連絡接触有無
   - 委託有無
   - 提供有無
   - 保管（場所、方法、期限）
   - 処分区分

   「個人情報管理台帳」は、作成日、作成者、承認日、承認者等を明確にし、最新性を維持する。
5) 新規の種類の個人情報を取得する場合は、「個人情報取扱申請書」により、個人情報の項目、利用目的、保管方法、利用期限、保管期限、件数等を明確にして保護管理者に申請し承認を得る。なお、「個人情報取得申請書」により取得した新規の種類の個人情報は、随時「個人情報管理台帳」に登録し、保護管理者の承認を得る。

A.3.3.2　法令、国が定める指針その他の規範

(1) 健康推進機構は、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参照できる手順を確立し、かつ、維持する。

(2) 健康推進機構は、自らの業務に関連のある範囲で、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「個人情報関連法規一覧表」に特定し、社内イントラネット等で従業者全員が参照

できる措置を講じる。

(3) 法令、国が定める指針その他の規範は、個人情報保護委員会、及び関係省庁、取引のある地方自治体、業界団体のホームページ等を参照し、半年１回（4 月、10 月）定期的に見直し、更新を行う。

(4) 新たな業務、取引等が発生し、関連する法令、国が定める指針、その他業界のガイドライン、取引先の要求等を追加する必要が出てきた場合は、随時「個人情報関連法規一覧表」を更新する。

(5) 特定し、更新した「個人情報関連法規一覧表」は、更新日付を明確にし、保護管理者の承認を得て、最新性を維持する。また、「個人情報関連法規一覧表」は、社内イントラネットで閲覧可能な措置を講じるものとする。なお、以下の法令、ガイドラインはＰＭＳを運営していく上で必須の規範とする。

1) 「個人情報の保護に関する法律」
2) 「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）」
3) 「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」
4) 「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）」
5) 「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について」
6) 「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に関する法律」
7) 「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」
8) 「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ドライン（厚生労働省）」

A.3.3.3 リスクアセスメント及びリスク対策

(1) 健康推進機構は、**A.3.3.1** によって特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持する。

(2) 健康推進機構は、**A.3.3.1** によって特定した個人情報について、その取り扱いの各局面（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄にいたる一連の流れにおける各局面）における個人情報保護リスク（個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響のおそれ）を認識し、分析し、必要な対策を講じるため、以下の手順を確立し、維持する。

1) リスクアセスメントは、個人情報の特定後、特定された個人情報の取扱いを考慮し、個人情報単位に、取り扱いに類似性がある場合はグルーピングした個人情報単位、及び取り扱う媒体の違い等により分類した個人情報単位に「リスクアセスメント表」を用いて行う。
2) 定期的なリスクアセスメントは、取り扱う部門、個人情報ごとに部門管理責任者が４月に実施する。
3) 新たな事業により、取り扱う個人情報が増えた場合や、取り扱う環境等に大きな変更があった場合、もしくは事件事故等を起こした場合は、随時リスクの見直しを行い「リスクアセスメント表」を更新する。
4) 「リスクアセスメント表」には、個人情報もしくはグループ化した個人情報名、取扱いの局面、認識したリスク、リスク対策、対策を反映すべき規程、残留リスク等の管理項目と、リスク対策の実施状況、残留リスクの顕在化の有無等を内部監査で点検するためのチェック項目欄を設ける。
5) リスクアセスメントは、個人情報もしくはグループ化した個人情報別に、取得・入力から消去・

廃棄にいたるライフサイクルの局面ごとに、リスクを認識し、認識したリスクに対する実施すべき対応策を決定し、対応策を反映すべき具体的な規程を設定する。対策をとっても依然として残るリスク、及び多額の投資等が必要となり経済的に対策を取れないために残るリスクを残留リスクとして管理する。

6) 部門毎に実施した「リスクアセスメント表」は、保護管理者が集約し、取り扱いの局面の漏れがないか、リスク対策、残留リスクの認識の妥当性等を検証し、理事長に提出し承認を得る。

7) 理事長は対策に対する費用対効果などを総合的に勘案し、問題がある場合は、保護管理者に見直しを指示する。

8) 「リスクアセスメント表」の“リスク対策”及び“残留リスク”は、内部監査において実施状況、リスク対策の妥当性、及び残留リスクの顕在化の有無について検証する。リスク対策の妥当性が低い場合や、残留リスクの顕在化の兆候が見受けられた場合は、リスクアセスメントにフィードバックを行い継続的な改善につなげる。

A.3.3.4 資源、役割、責任及び権限

(1) 理事長は、ＰＭＳを確立し、実施し、維持し、かつ、改善するために不可欠な資源を用意するものとする。理事長に事故あるときは、副理事長がその事務を代決する。

(2) 理事長は、ＰＭＳを効果的に実施するために、役割、責任及び権限を定め、文書化し、かつ、従業者に周知する。

(3) 理事長は、『個人情報保護マネジメントシステム－要求事項（JIS15001:2017)』の規格の内容を理解し実践する能力のある保護管理者を事業者の内部の者から指名し、ＰＭＳの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせる。

(4) 保護管理者は、ＰＭＳの見直し及び改善の基礎として、理事長にＰＭＳの運用状況を報告しなければならない。

(5) 理事長は、公平、かつ、客観的な立場にある監査責任者を事業者の内部の者から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行なわせなければならない。

(6) 監査責任者は、監査を指揮し、監査報告書を作成し、理事長に報告し、また、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しなければならない。

(7) 監査責任者と保護管理者とは異なる者でなければならない。

健康推進機構はＰＭＳを実施するための体制として、以下の担当を定め、ＰＭＳの実施体制は、「個人情報保護体制図」により、従業者に周知する。

役職名	役割・責任及び権限
個人情報保護管理者	理事長によって健康推進機構の内部から指名された者であって、ＰＭＳの実施及び運用に関する責任及び権限をもつ者。
個人情報保護監査責任者	理事長によって健康推進機構の内部から指名された者であって、公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。健康推進機構では事業部長とする。
監査員	健康推進機構の内部の監査責任者によって指名された者であって、監査責任者の指示に従い内部監査を実施する。但し、自らが所属する部

	門の監査を実施することは出来ない。
個人情報保護教育責任者	ＰＭＳに関する教育を実施する者で、教育の計画、実施、記録の保管等の責任を負う。健康推進機構では総務部長とする。
苦情及び相談責任者(開示含む)	健康推進機構の個人情報及びＰＭＳに対する苦情及び、開示等の要求に対応する窓口では総務課長がこの任に当たる。
個人情報保護部門管理責任者	個人情報保護管理者によって健康推進機構の内部の各部門から指名された者であって、各部門のＰＭＳの実施及び運用に関する責任及び権限をもつ者。
事務取扱担当者	番号法の規定により、個人番号利用事務に関して行われる個人番号を必要な限度で利用し、処理する事務を行う担当者。
情報システム責任者	個人情報保護管理者によって健康推進機構の内部の各部門から指名された者であって、情報システム及びネットワークの運用及び管理に関する責任及び権限をもつ者。
ストレスチェック実施責任者	心理的な負担の程度を把握するための検査等実施要綱を職員に配布又は掲示板等に掲載することにより、ストレスチェック制度の趣旨等を職員に周知する。
ストレスチェック実施事務従事者	ストレスチェックの質問票の入力や保管、結果の出力や記録の保存を行う。
事務局責任者	個人情報保護管理者によって健康推進機構の内部の各部門から指名された者であって、個人情報保護管理者の指示に従いＰＭＳの年間計画の策定と各部門への指示及び指導を実施する。

A.3.3.5　内部規程

(1) 健康推進機構は、次の事項を含む内部規程を文書化し、かつ、維持する。また、内部規程の改定、管理、維持の責任者は、保護管理者とする。

a) 個人情報を特定する手順に関する規定（本規程 A.3.3.1）

b) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定（本規程 A.3.3.2）

c) 個人情報に関するリスクの認識、分析及び対策の手順に関する規定（本規程 A.3.3.3）

d) 健康推進機構の各部門及び階層における個人情報を保護するための権限及び責任に関する規定（本規程 A.3.3.4）

e) 緊急事態（個人情報が漏えい、滅失又はき損をした場合）への準備及び対応に関する規定（本規程 A.3.3.7）

f) 個人情報の取得、利用及び提供に関する規定（本規程 A.3.4.2）

g) 個人情報の適正管理に関する規定（本規程 A.3.4.3、安全管理規程）

h) 本人からの開示等の請求等への対応に関する規定（本規程 A.3.4.4）

i) 教育などに関する規定（本規程 A.3.4.5）

j) 文書化した情報の管理に関する規定（本規程 A.3.5）

k) 苦情及び相談への対応に関する規定（本規程 A.3.6）

l) 点検に関する規定（本規程 A.3.7）

m) 是正処置に関する規定（本規程 A.3.8）

n) マネジメントレビューに関する規定（本規程 A.3.7.3）

o) 内部規程の違反に関する罰則の規定（本規程 A.3.4.3.3、就業規則第 46 条）

※安全管理措置はＰＭＳ全体で担保する。

(2) 健康推進機構は、事業の内容に応じて、ＰＭＳが確実に適用されるよう規程を改定する。

A.3.3.6 計画策定

(1) 健康推進機構は、ＰＭＳを確実に実施するために必要な教育、監査等の計画を立案し、文書化し、かつ、維持する。

a) 毎年期首に、教育責任者は全従業者に対してＰＭＳの教育を実施するための「ＰＭＳ教育計画書」を作成しなければならない。当計画書は保護管理者の承認を得て、全従業者に周知するとともに保護管理者が保管し、文書管理を行う。

b) 毎年期首に、監査責任者は「ＰＭＳ内部監査計画書」を作成しなければならない。当計画書は理事長の承認を得て全従業者に周知するとともに、監査責任者が保管し、文書管理を行う。

A.3.3.7 緊急事態への準備

(1) 健康推進機構は、緊急事態を特定するための手順、また、それらについてどのように対応するかの手順を確立し、実施し、かつ、維持する。

(2) 健康推進機構は、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の手順を確立し、かつ、維持する。

(3) 健康推進機構は、緊急事態が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持する。

a) 漏えい、滅失又はき損が発生した個人情報の内容を、個人情報から識別される本人（以下、「本人」という。）に速やかに通知するか、又は本人が容易に知り得る状態に置くこと。

b) 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、発生原因及び対応策を、遅滞なく公表すること。

c) 事実関係、発生原因及び対応策を関係機関に直ちに報告すること。

(4) 緊急事態の特定、初期対応、対応手順等については、以下のとおりとする。

1) 緊急事態の特定

取り扱う個人情報の漏えい、滅失又はき損、セキュリティ等に関するインシデントが発生した場合、本人、委託者への影響度に応じ、個人情報リスク分類表に基づき「緊急事態」の特定を行う。

個人情報リスク分類表

分類	状態
レベルＡ	個人情報に関して、インシデントが発生し、確認のうえ取り扱う個人情報の漏えい、滅失又はき損等本人又は、委託者へ影響がない場合「緊急事態」としない。

レベルＢ	個人情報に関して、インシデントが発生し、確認のうえ取り扱う個人情報の漏えい、滅失又はき損等本人又は、委託者へ影響がある場合「緊急事態」とする。
レベルＣ	レベルＢで「緊急事態」に特定され、個人情報保護規程 A.3.3.7 （4）-3）-⑤-3 に該当する事故等が発生した場合。

2） 緊急事態への初期対応

①緊急事態に遭遇し、又は把握した場合の初期対応については、リスクマネジメント・危機管理に関する規程　第 10 条（事故等発覚後の危機管理）に基づき対応する。

②保護管理者は、直ちに「緊急連絡網」に従って、関係者への連絡を行う。

③保護管理者は、危機管理対策本部の設置について、リスクマネジメント・危機管理に関する規程第 11 条（危機管理対策本部の設置）に基づき対応する。

3）緊急事態への対応手順

①保護管理者は、発生した緊急事態についての事実関係を確認し、確認でき次第状況を「事故報告書」にて、代表者に報告する。

②保護管理者、及び危機管理対策本部のメンバーは、緊急事態の被害を最小限に抑えるための対応（当該個人情報の利用・提供の停止、関連部門・委託先への適切な指示など）を行う。

③保護管理者は、個人情報の事故等の状況について本人に速やかに通知する。又は本人が容易に知り得る状況に置くために、ホームページに公表する。

なお、個人情報の取扱いの全部又は一部を受託している場合は、委託者と相談のうえ実施する。

④二次災害の防止、類似事案の発生回避等の観点から、可能な限り事実関係、発生原因及び対応策等を、遅滞なくホームページに公表する。公表する責任者は、保護管理者とし、以下の関係機関に直ちに報告する。

－取引先等の利害関係企業

－警察

－審査を受けた機関：一般社団法人医療情報システム開発センター（ＭＥＤＩＳ-ＤＣ）

－認定個人情報保護団体：一般財団法人日本情報経済社会推進協会（ＪＩＰＤＥＣ）

－個人情報保護委員会

⑤一般社団法人医療情報システム開発センター（以下「関係審査機関」とする。）及び個人情報保護委員会（以下「委員会」とする。）に提出する「事故報告」について次のとおりとする。

1. レベルＡに分類された場合は、関係審査機関、委員会へ「事故報告」の提出は必要ないものとする。

2. レベルＢに分類された場合は、発覚した日から３０日以内（不正の目的をもって行われたおそれがある漏えいの場合は、６０日以内）に関係審査機関へ「事故報告」を提出する。

3. 次の事項に該当する事故等が発生した場合は、レベルＣに分類し、５日以内に「速報」として関係審査機関、及び委員会へ「事故報告」を提出する。

Ⅰ.要配慮個人情報の漏えい等、又は発生したおそれがある場合
Ⅱ.不正に利用されることにより財産的被害が生じるおそれがある事故等、又は発生したおそれがある場合
Ⅲ.不正の目的をもって行われたおそれがある事故等、又は発生したおそれがある場合
Ⅳ.個人データに関わる本人の数が１，０００人を超える事故等が発生し、又は発生したおそれがある場合
Ⅴ.付与機関がＰマーク審査基準における重大な違反、又は違反のおそれがあると認めた場合
Ⅵ.マイナンバーが情報提供ネットワークシステム等からの漏えい、滅失、き損した場合
Ⅶ.マイナンバーを不特定多数の者に閲覧された場合
Ⅷ.マイナンバーの不正の目的による漏えい、滅失、き損した場合
Ⅸ.マイナンバーの事故が１００人を超える場合

事故報告書提出先	報告種別	個人情報リスク分類		
		レベルＡ	レベルＢ	レベルＣ
関係審査機関 （一般社団法人医療情報システム開発センター）	事故報告（速報）	×	×	○
	事故報告	×	○	○
委員会 （個人情報保護委員会）	事故報告（速報）	×	×	○
	事故報告	×	×	○

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。
なお、個人情報の取扱いの全部又は一部を受託している場合は、委託者と相談のうえ実施する。
⑦再発防止のため、緊急事態が沈静化した後に、是正処置により、原因を特定し事故の原因を根本的に除去する処置をとる。また、リスクアセスメントにフィードバックし、リスク対策、及び残留リスクを見直し、見直したリスク対策の実施状況、残留リスクの顕在化の兆候の有無等を内部監査で点検する。

A.3.4　実施及び運用

A.3.4.1 運用手順

健康推進機構は、ＰＭＳを確実に実施するために、運用の手順を確立するものとする。

A.3.4.2　取得、利用及び提供に関する原則

A.3.4.2.1　利用目的の特定

(1) 個人情報を取り扱うにあたり、その利用目的をできる限り特定し、その利用目的の達成に必要な範囲内において行う。
(2) 利用目的の特定にあたり、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するよう配慮する。
(3) 新規の種類の個人情報を取得する場合は、「個人情報取扱申請書」にて利用目的を明確にし、保護

管理者の承認を得る。なお、取得した個人情報は「個人情報管理台帳」に特定し、利用目的を明確にする。

A.3.4.2.2　適正な取得

健康推進機構は、適法、かつ、公正な手段によって個人情報を取得するものとする。

(1) 第三者から A.3.4.2.4 により個人情報を取得する場合（受託による取得を含む）、提供元又は委託元が個人情報を適正に取り扱っていることを、提供、又は受託を受ける前に事前に確認し、委託契約に適正な取得に関する条項を盛り込むか、担当者等に確認を行い、打ち合わせ議事録等に適正な取得の確認の記録を残す。

(2) 提供者又は委託者が明らかに法令等に違反している場合には、提供又は委託を受けてはならない。

A.3.4.2.3　要配慮個人情報

(1) 健康推進機構は、新たに要配慮個人情報を取得する場合、あらかじめ書面による同意を得ないで、要配慮個人情報を取得しない。ただし、次に掲げるいずれかに該当する場合には、書面による本人の同意を得ることを要しない。

a) 法令に基づく場合

b) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

c) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

d) 国の機関若しくは地方公共団体又はその委託を受けた者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、本人の同意を得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とき

e) その他、個人情報取扱事業者の義務などの適用除外とされている者及び個人情報保護委員会規則で定めた者によって公開された要配慮個人情報、又は政令で定められた要配慮個人情報であるとき

(2) 前項ただし書きにより、例外的に要配慮個人情報を取得、利用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。また、ただし書き a)～d) を適用して、提供する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

(3) 取得、利用、提供する要配慮個人情報の種類、利用目的を明確にした「個人情報の取扱いに関する同意書」により本人から同意を得るものとする。

A.3.4.2.4　個人情報を取得した場合の措置

(1) 健康推進機構は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかにその利用目的を、本人に通知するか、又は公表する。ただし、次に示すいずれかに該当する場合は、この限りではない。

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

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

(2) 個人情報を取得及び取得後の際の措置は、以下のとおりとする。

1) 新規の種類の個人情報を取得する場合は、事前に「個人情報取扱申請書」により申請し、保護管理者の承認を得る。

2) 個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかにその利用目的をホームページで公表する。

3) ただし書き a)～d)を適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

4) ただし書き d)を拡大解釈して、利用目的を通知、公表することなく取得、利用してはならない。ただし書き d)の適用は、一般慣行としての名刺交換、入退管理のための来訪者の記録、見積書、請求書などの伝票に記載された住所、担当者氏名等に極力限定する。

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

(1) 健康推進機構は、A.3.4.2.4 の措置を講じた場合において、本人から、書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）に記載された個人情報を直接に取得する場合には、少なくとも、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、書面によって本人に明示し、本人の同意を得る。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合、A.3.4.2.4 のただし書き a)～d)のいずれかに該当する場合は、本人の同意を得ることを要しない。

a) 事業者の氏名又は名称

b) 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

c) 利用目的

d) 個人情報を第三者に提供することが予定されている場合の事項

- 第三者に提供する目的
- 提供する個人情報の項目
- 提供の手段又は方法
- 当該情報の提供を受ける者又は提供を受ける者の組織の種類、及び属性
- 個人情報の取扱いに関する契約がある場合はその旨

e) 個人情報の取扱いの委託を行うことが予定される場合には、その旨

f) A.3.4.4.4～A.3.4.4.7 に該当する場合には、その求めに応じる旨及び問合せ窓口

g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果

h) 本人が容易に認識できない方法によって個人情報を取得する場合には、その旨

(2) 本人から直接書面により取得する場合の措置は、以下のとおり。

1)　直接書面により、新規の種類の個人情報を取得する場合は、事前に「個人情報取扱申請書」により申請し、保護管理者の承認を得る。

2)　取得に際しては、本人に対して、上記 a)～h)の事項を書面により明示し、書面による同意を得る。

①採用応募時

ホームページから「個人情報の取扱いに関する同意書（採用応募者)」をダウンロードし、記入してもらい、応募書類と共に送付してもらうことにより明示的な同意を得る。

②採用従業者

入職手続きの際に「個人情報の取扱いに関する同意書（従業者)」を記入し、入職手続き時に取得する書類と共に提出してもらうことによって明示的な同意を得る。

③ウェブからの取得時

ウェブからの個人情報の取得は、上記 a)～h)の項目を明示した「個人情報の取扱いについての同意事項」画面に同意ボタンを設け、同意ボタンを押下した場合に同意を得たものとみなし、個人情報の登録を行う入力画面が開くような画面遷移の構造とし、明示的な同意を得た場合のみ登録できるものとする。

3)　ただし書きを適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

4)　職員等の個人情報の収集、利用する場合の措置及び手続きの詳細については、「職員等の個人情報保護規程」による。

5)「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（以下「番号法（マイナンバー法)」という。)」と、特定個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン（事業者編)」に基づき、健康推進機構の取り扱う特定個人情報等の適正な取扱いについては、「特定個人情報取扱規程」による。

A.3.4.2.6　利用に関する措置

(1) 健康推進機構は、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するものとする。

(2) 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)に示す事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得なければならない。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合は、本人の同意を得ることを要しない。

(3) 利用目的の必要な範囲を超えて個人情報を利用する場合の措置は、以下のとおり。

1)　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「個人情報取扱申請書」により申請し、保護管理者の承認を得る。

2)　利用目的を変更する場合、あらじめ、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を「個人情報取扱い同意書面」に記載して本人に通知し、本人の同意を得る。

3)　ただし書き A.3.4.2.3 の a)～d)を適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

4)　目的外利用に該当するかどうか判断に迷う場合は、保護管理者に判断を求める。

A.3.4.2.7　本人に連絡又は接触する場合の措置

(1) 健康推進機構は、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)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、本人の同意を得るものとする。ただし、次に示すいずれかに該当する場合は、本人に通知し、本人の同意を得ることを要しない。

a) 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を明示又は通知し、既に本人の同意を得ているとき

b) 個人情報の取扱いの全部又は一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき

c) 合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する事業者が、既に 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を明示又は通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき

d) 個人情報が特定の者との間で共同して利用され、共同利用者が、既に 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を明示又は通知し、本人の同意を得ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき（以下、「共同利用」という。）

- 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

e) A.3.4.2.4 のただし書き d)に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人に連絡又は接触するとき。

f) A.3.4.2.3 のただし書き a)～d)のいずれかに該当する場合。

(2) 個人情報を利用して本人に連絡又は接触する場合の措置は、以下のとおり。

1) 本人に連絡又は接触する場合は、事前に「個人情報取扱申請書」により申請し、保護管理者の承認を得る。

2) 本人に連絡又は接触する場合は、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、本人の同意を得る。取得方法には、その個人情報の出所は何か（卒業生名簿、電話帳、登記簿等の「取得源」）、どのように取得したのか（書店から購入した、提供を受けたなどの「取得の経緯」）の両方を記述する。

※連絡又は接触手段ごとに、本人への通知、同意を得る方法

①電話

口頭で、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、本人の同意を得る。

②ＦＡＸ

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、及び取得方法を記載した「個

人情報取扱い同意書面」を同時に送信し、同意書に記名して返信してもらうことにより本人の同意を得る。

③電子メール

連絡又は接触する前に、「個人情報取扱い同意書面」を添付ファイルにて送信し、同意のサインを記入し返信してもらう。同意を得られた場合のみ、アクセスすることが出来る。

3) ただし書き b)～f)を適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

4) ただし書き d)を適用する共同利用の場合にはあらかじめ、本人に通知し、又は本人が容易に知り得る状態に置く項目を、ホームページに公表し、本人が容易に知り得る状態に置く。

A.3.4.2.8 個人データの提供に関する措置

(1) 健康推進機構は、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、取得方法及び A.3.4.2.5 の a)～d)に示す事項又はそれと同等以上の内容の事項を通知し、本人の同意を得るものとする。ただし、次に示すいずれかに該当する場合は、本人に通知し、本人の同意を得ることを要しない。

a) A.3.4.2.5 又は A.3.4.2.7 の規定によって、既に A.3.4.2.5 の a)～d)に示す事項又はそれと同等以上の内容の事項を本人へ明示又は通知し、本人の同意を得ているとき

b) 本人の同意を得ることが困難な場合であって、法令等が定める手続に基づいた上で、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知するか、又はそれに代わる同等の措置を講じているとき

1) 第三者への提供を利用目的とすること
2) 第三者に提供される個人データの項目
3) 第三者への提供の手段又は方法
4) 本人の請求などに応じて当該本人が識別される個人データの第三者への提供を停止すること
5) 取得方法
6) 本人からの請求などを受け付ける方法

c) 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、法令に基づき又は本人若しくは当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって、b)の 1)～6)で示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知するか、又は本人が容易に知り得る状態においているとき

d) 特定した利用目的の達成に必要な範囲内において、個人データの取扱いの全部又は一部を委託するとき

e) 合併その他の事由による事業の承継に伴って個人データを提供する場合であって、承継前の利用目的の範囲内で当該個人データを取り扱うとき

f) 個人データを共同利用している場合であって、共同して利用する者の間で、A.3.4.2.7 に規定する共同利用について契約によって定めているとき

g) A.3.4.2.3 のただし書き a)～d)のいずれかに該当する場合

(2) 個人情報を第三者に提供する場合の措置は、以下のとおり。

1) 個人データを第三者に提供する場合は、事前に「個人情報取扱申請書」により申請し、保護管理者の承認を得る。
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、取得方法及び A.3.4.2.5 の a)～d)に示す事項又はそれと同等以上の内容の事項を「個人情報の取扱い同意書面」で通知し、本人の同意を得る。
3) ただし書き b)～g)を適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。なお、捜査機関から照会や事情聴取に係る提供の際は、成りすましを防ぐため当該情報提供を求めた捜査官の役職、氏名等（本人確認可能な書面の提出、あるいは、捜査関係事項書類の提出を求める）、提供内容、任意捜査か否か等の情報を確認する。
4) 原則的に、ただし書き b)を適用しない。
5) ただし書き c)を適用する場合は、b)の 1)～6)で示す事項又はそれと同等以上の内容の事項を、ホームページで公表し、本人が容易に知り得る状態におくものとする。
6) ただし書き f)を適用する共同利用の場合にはあらかじめ、本人に通知し、又は本人が容易に知り得る状態に置く項目を、ホームページに公表し、本人が容易に知り得る状態に置くとともに、共同利用者との間で、A.3.4.2.7 に規定する共同利用についての契約によって定めるものとする。

A.3.4.2.8.1 外国にある第三者への提供の制限

(1) 健康推進機構は、法令等の定めに基づき、外国にある第三者に個人データを提供する場合には、あらかじめ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るものとする。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合及びその他法令等によって除外事項が適用される場合には、本人の同意を得ることを要しない。

(2) 外国にある第三者への提供を行う場合の措置は、以下のとおり。

1) 個人データを外国にある第三者に提供する場合は、事前に「個人情報取扱申請書」により申請し、保護管理者の承認を得る。
2) 個人データを外国にある第三者に提供する場合には、あらかじめ、本人に対して、外国にある第三者への提供を認める旨の事項を明確にした同意書面で通知し、本人の同意を得る。
3) ただし書き適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

A.3.4.2.8.2 第三者提供に係る記録の作成など

(1) 健康推進機構は、個人データを第三者に提供したときは、法令等の定めるところによって記録を作成し、保管するものとする。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、又は次に示すいずれかに該当する場合は、記録の作成を要しない。

a) 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合
b) 合併その他の事由による事業の承継に伴って個人データが提供される場合
c) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利

用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知するか、又は本人が容易に知り得る状態においているとき。

(2) 第三者提供に係わる記録を作成する場合の措置は、以下のとおり。

1) 保護管理者は、個人データを第三者に提供した場合は、「個人データ第三者提供記録」を作成し、当該記録を作成した日から、法令等で定める保存期間保存する。「個人データ第三者提供記録」には次に示す項目を含める。

－当該個人データを提供した年月日

－当該第三者の氏名又は名称

－その他の法令等で定める事項に関する記録の作成

2) ただし書き適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

A.3.4.2.8.3　第三者提供を受ける際の確認など

(1) 健康推進機構は、第三者から個人データの提供を受けるに際しては、法令等の定めるところによって確認を行う。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、又は A.3.4.2.8.2 の a)～c)のいずれかに該当する場合は、確認を要しない。

(2) 第三者提供を受ける際は、法令等の定めるところによって確認の記録を作成、保管する。

1) 保護管理者は、第三者から個人データの提供を受けるに際しては、「個人データ第三者提供受領記録」を作成し、次に示す項目を確認し記録する。

－提供元である第三者の氏名又は名称及び住所並びに法人などについては代表者の氏名

－提供元である第三者による当該個人データの取得の経緯

2) ただし書きを適用する場合は、事前に「個人情報例外適用申請書」にて申請し、保護管理者の承認を得る。

A.3.4.2.9　匿名加工情報

(1)　健康推進機構は、現行では匿名加工情報の取扱いを行わないものとする。取り扱う場合は、リスクアセスメント及びリスク対策を実施し、その結果を考慮して方針を定める。

A.3.4.3　適正管理

A.3.4.3.1　正確性の確保

(1) 健康推進機構は、利用目的の達成に必要な範囲内において、個人データを、正確、かつ、最新の状態で管理する。

(2) 個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去・廃棄するよう努める。消去・廃棄の結果は「個人情報廃棄記録簿」に記録する。

(3) 個人情報入力時の照合・確認及び保管等の措置については、以下のとおり。

1)　個人情報の入力時の照合・確認

個人情報を入力する場合は、入力した個人情報の入力原票との照合及び確認を、複数体制で実施

する。

2) 保管期限の設定

取扱う個人データの保管期限は、受託業務等においては、契約で定めた期間、従業者情報等においては、法定保存期限が定められているものはそれに従う。個々の個人情報については「個人情報管理台帳」の“保管期限”欄に記載し、管理する。

A.3.4.3.2 安全管理措置

(1) 健康推進機構は、取り扱う個人情報の個人情報保護リスクに応じて、漏えい、滅失又はき損の防止その他の安全管理のために、必要、かつ、適切な措置を講じるものとする。

(2) 健康推進機構は、リスクアセスメント及びリスク対策（**A.3.3.3**）において講じることとした対策を、安全管理措置に反映する。

(3) 健康推進機構は、物理的安全管理措置及び技術的安全管理措置を「安全管理規程」に規定する。
なお、「安全管理規程」はリスクアセスメント時期と連動し見直しを行なう。

A.3.4.3.3 従業者の監督

(1) 健康推進機構は、従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対し、必要、かつ、適切な監督を行うものとする。

1) 従業者との雇用契約時に、又は委託契約時に個人情報の非開示条項を盛り込んだ「誓約書」を締結する。又は、就業規則に業務上知り得た情報の非開示の義務を規定する。

2) 「誓約書」に、非開示条項は、契約終了後も一定期間有効であるよう定める。又は、就業規則に業務上知り得た情報の非開示の義務が一定期間有効であるよう定める。

3) ＰＭＳに違反した場合は、「就業規則」の懲戒条項を適用する。

4) 健康推進機構は、盗難防止のため監視カメラを設置し、従業員及び入館者のモニタリングを実施する。

－監視カメラの設置場所には「監視カメラ稼働中」の標札を貼付する

－監視カメラによるモニタリングの実施、及び画像の保管の責任者は、総務部長とする

－監視カメラによるモニタリングの実施状況については、適正に行なわれているか内部監査又は運用の確認で検証する

A.3.4.3.4 委託先の監督

(1) 健康推進機構は、個人データの取扱いの全部又は一部を委託する場合は、十分な個人情報の保護水準を満たしている者を選定する。このため、委託を受けるものを選定する基準には、少なくとも委託する当該業務に関して、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ことを含める。

(2) 健康推進機構は、個人データの取扱いの全部又は一部を委託する場合は、委託する個人情報の安全管理が図られるよう、委託を受けた者に対する必要、かつ、適切な監査を行う。

(3) 健康推進機構は、次に示す事項を契約によって規定し、十分な個人情報の保護水準を担保するものとする。

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、およ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

健康推進機構は、当該契約書などの書面を個人データの保有期間にわたって保存する。

(4) 健康推進機構は、個人番号、特定個人情報を委託する場合は、上記の a)～h)に加えて、秘密保持義務、従業者に対する監督・教育等の条項を含んだ契約書により契約を締結するものとする。

(5) 委託先選定に係わる基準、評価等については、以下のとおりとする。

1) 委託先選定基準を定める手順

① 委託先を選定、評価するための基準を作成する。

② 委託先の選定基準は、個人データの取扱いを含むか、若しくは個人データに触れる可能性があるかによって評価項目を設定する。

≪個人データの取扱いを含む場合≫

以下の評価項目を含む「委託先評価表」にて選定評価を行う。

－プライバシーマークを取得しているか

委託先がプライバシーマークを取得していれば、委託先の選定評価基準に合格とし、以下の選定評価項目は適用しない

－個人データに関するインシデント（事件・事故）が発生していないか
－組織的安全管理措置の実施状況
－人的安全管理措置の実施状況
－物理的安全管理措置の実施状況
－技術的安全管理措置の実施状況

ただし、取り扱う個人データによって、すべての項目を一律に評価する必要はないが、必須の評価項目については、確実に安全管理措置が実施され、個人データの保護が担保されているという評価が必要である。

≪個人情報に触れる可能性がある場合≫

立ち入ることのできる範囲の制限、業務上知り得る情報についての守秘義務の契約書を取り交わしているか。

③ 委託先選定基準は、定期的な再評価の実施前、通常は３月に見直す。

2) 委託先の評価

① 個人データを取扱う業務の委託先あるいは、施設内に立ち入り個人情報に触れる可能性のある委託先について、毎年４月に「委託先一覧表」に洗い出す。

② 新たに個人情報を取り扱う業務を委託する場合は、委託開始前に「委託先評価表」を使用して、委託先の選定評価を行う。取り扱う個人情報によって、「委託先評価表」のすべての項目を一律

に評価する必要はないが、該当する委託業務について、自社と同等以上の個人情報保護の水準にあることが望ましい。評価が選定基準に満たない項目については、改善要求を行い改善実施の確認後に、委託する。「委託先評価表」は保護管理者の承認を得る。

③ 「委託先一覧表」で管理している委託先のうち、継続的に委託する委託先については、毎年定期的に、4月に再評価を実施する。また、緊急事態の発生等の場合は、随時再評価を行う。

3) 委託業務を開始する前に、a)～h)の内容を盛り込んだ「委託業務契約書」により委託先と契約を締結する。

b)項の個人情報の安全管理に関する事項には、以下の事項を含める。

- 個人情報の漏えいの防止、盗用禁止に関する事項
- 委託範囲外の加工、利用の禁止
- 委託契約範囲外の複写、複製の禁止
- 委託契約期間
- 委託契約終了後の個人情報の返還・消去・廃棄に関する事項

c)項の再委託に関する事項には、以下の項目を含める

- 再委託を行うに当たっての委託者への文書による報告

相手先契約書や、約款によりサービスを提供し個別契約に応じない場合等で、a)～h)のすべての項目を盛り込んだ契約が締結できない場合は、必要に応じて不足している項目について残留リスクとして把握し管理する。

4) 委託先と締結した業務委託契約書は、個人データの保有期間にわたって保有する。

A.3.4.4 個人情報に関する本人の権利

A.3.4.4.1 個人情報に関する権利

(1) 健康推進機構は、保有個人データ、本人から開示等の請求等を受けた場合は、A.3.4.4.4～A.3.4.4.7の規定によって、遅滞なくこれに応じるものとする。ただし、次のいずれかに該当する場合は、保有個人データにはあたらない。

a) 当該個人データの存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの

b) 当該個人データの存否が明らかになることによって、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もの

c) 当該個人データの存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの

d) 当該個人データの存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序維持に支障が及ぶおそれのあるもの

(2) 健康推進機構は、保有個人データに該当しないが、本人から求められる利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求などの全てに応じることができる権限を有する個人情報についても、保有個人データと同等に取り扱うものとする。

(3) (1) のただし書きを適用する場合は、「個人情報開示等請求回答書」にて申請し、保護管理者の承認を得るものとする。

A.3.4.4.2　開示等の請求等に応じる手続

(1) 健康推進機構は、開示等の請求等に応じる手続きとして次の事項を定める。

a) 開示等の請求等の申出先

b) 開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式

c) 開示等の請求等をする者が、本人又は代理人であることの確認の方法

d) A.3.4.4.4 又は A.3.4.4.5 による場合の手数料（定めた場合に限る。）の徴収方法

(2) 健康推進機構は、本人からの開示等の請求等に応じる手順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配慮する。

(3) 健康推進機構は、A.3.4.4.4 又は A.3.4.4.5 によって本人からの開示等の請求等に応じる場合に、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、その額を定める。

(4) 開示等の請求手続き等については、以下のとおりとする。

1) 開示等の請求等の申出先

苦情相談窓口が開示等の求めを受け付ける。

2) 提出すべき書面及び開示等の請求等の方式

「個人情報開示等請求回答書」によって行う。請求書面は、健康推進機構のホームページからダウンロードできるようにする。請求等は郵送又は直接持参によって行う。なお、回答は「個人情報開示等請求回答書」にて行う。

3) 開示等の請求等をする者の確認方法

本人確認のための書類として“運転免許証”、“健康保険証”等の写しを提出していただく。代理人の場合は、「委任状」と本人確認のための“運転免許証”、“健康保険証”等の写しを提出していただく。

個人番号・特定個人情報の場合は、“個人番号カード”、もしくは“通知カード”＋“本人の身元確認書類”の写しを提出していただく。

なお、本人確認のための書面に、本籍地等が記載されている場合は、黒塗りしてマスキングするなどの要配慮個人情報対策を実施のうえ、提出していただく。

4) 開示対象個人情報の利用目的の通知、開示の場合、開示等の請求手数料は発生しないが、郵送する場合において、返信用郵送料として手数料相当額の郵便切手を同封していただくか若しくは同等の手段を講じる。

A.3.4.4.3　保有個人データに関する事項の周知など

(1) 健康推進機構は、当該保有個人データに関し、次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。）に置く。

a) 組織の氏名又は名称

b) 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。

c) 全ての保有個人データの利用目的。[A.3.4.2.4 の a)～c)までに該当する場合を除く。]

d) 保有個人データの取扱いに関する苦情の申出先。

e) 当該組織が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先。

f) A.3.4.4.2 によって定めた手続。

(2) 健康推進機構は、開示対象個人情報に関する上記 a)～f)の事項をホームページに掲示し周知する。

A.3.4.4.4 保有個人データの利用目的の通知

(1) 健康推進機構は、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には、遅滞なくこれに応じる。ただし、A.3.4.2.4 のただし書き a)～c)のいずれかに該当する場合、又は A.3.4.4.3 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は利用目的の通知を必要としないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

1) 本人への回答内容（求めに応じない場合を含む。）に関しては、「個人情報開示等請求回答書」に記載し、同回答書により保護管理者の承認を得る。

2) ただし書きにより利用目的を通知しない場合は、「個人情報開示等請求回答書」に適用したただし書きを明記し、保護管理者の承認を得る。

A.3.4.4.5 保有個人データの開示

(1) 健康推進機構は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。）の請求を受けたときは、法令の規定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、当該保有個人データを書面（開示の請求を行った者が同意した方法があるときは、当該方法）によって開示する。ただし、開示することによって次の a)～c)のいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明するものとする。

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) 健康推進機構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

(2) 個人保有データの開示については、以下のとおりとする。

1) 本人への回答内容（求めに応じない場合を含む。）に関しては、「個人情報開示等請求回答書」に記載し、同回答書により保護管理者の承認を得る。

2) ただし書きにより本人に開示しない場合は、「個人情報開示等請求回答書」に適用したただし書きを明記し、保護管理者の承認を得る。

A.3.4.4.6 保有個人データの訂正、追加又は削除

(1) 健康推進機構は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの訂正、追加又は削除（以下、この項において「訂正等」という。）の請求を受けた場合は、法令の規定によって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う。また、訂正等を行ったときは、その旨及びその内容を本人に対し遅滞なく通知し、訂正等を行わない旨の決定をしたときは、その旨及びその理由を本人に対し遅滞なく通知する。

1) 本人への回答内容（求めに応じない場合を含む。）に関しては、「個人情報開示等請求回答書」に記載し、同回答書により保護管理者の承認を得る。
2) 訂正等を行わない場合は、「個人情報開示等請求回答書」にその事由を明記し、保護管理者の承認を得る。

A.3.4.4.7　保有個人データの利用又は提供の拒否権

(1) 健康推進機構が、本人から当該本人が識別される保有個人データの利用の停止、消去又は第三者への提供の停止（以下、この項において「利用停止等」という。）の請求を受けた場合は、これに応じる。また、措置を講じた後は、遅滞なくその旨を本人に通知する。ただし、A.3.4.4.5 のただし書き a)～c) のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明するものとする。

1) 本人への回答内容（求めに応じない場合を含む。）に関しては、「個人情報開示等請求回答書」に記載し、同回答書により保護管理者の承認を得る。
2) ただし書きにより利用停止等を実施しない場合は、「個人情報開示等請求回答書」に適用したただし書きを明記し、保護管理者の承認を得る。

A.3.4.5　認識

(1) 健康推進機構は、すべての従業者に、定期的に少なくとも年１回以上の適切な教育を行い、関連する各部門及び階層における次の事項を認識させる手順を確立し、かつ、維持する。

また、個人番号を取扱う事務取扱担当者に対する教育も、年１回、適宜に行う。

a) 個人情報保護方針（内部向け個人情報保護方針及び外部向け個人情報保護方針）
b) 個人情報保護マネジメントシステムに適合することの重要性及び利点
c) 個人情報保護マネジメントシステムに適合するための役割及び責任
d) 個人情報保護マネジメントシステムに違反した際に予想される結果

(2) 教育責任者は、教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持する。

1) 教育の目的

従業者に、ＰＭＳを実施できるための力量を確実に身につけさせること。

2) 教育計画の作成

教育責任者は、毎年期首に「ＰＭＳ教育計画書」を作成し、保護管理者の承認を得て、電子掲示板等で従業者に周知する。また、当初計画した時期に実施できない場合は、「ＰＭＳ教育計画書」を見直し、再度保護管理者の承認を得て変更する。

また、「ＰＭＳ教育計画書」の作成と同時期に「ＰＭＳ教育受講対象者一覧表」を作成し、対象者

の管理を行う。

3) 教育教材の準備

教育用のテキストは、教育責任者が教育実施に合わせて準備する。教育テキストには上記 a)～ d)を含める。

4) 教育の実施

教育責任者は、教育計画に沿って、作成した教育テキストを使用して教育を実施する。

5) 理解度確認の実施

教育終了後、理解度確認を行うために「理解度確認テスト」を実施する。理解度が不足している者に対しては、フォローアップ教育を行う。

受講従業者別の教育受講日、理解度確認テストの結果等を「ＰＭＳ教育受講対象者一覧表」に記録する。

6) 教育実施記録の作成と保護管理者への報告

教育責任者は、「ＰＭＳ教育実施記録」を作成し、保護管理者に報告する。

7) 未受講者に対するフォローアップ教育

「ＰＭＳ教育受講者一覧表」で、予定している従業者が教育未受講の場合は、後日フォローアップ教育を実施する。長期休暇中等で計画期中に受講できない場合は，その事由を明記しておく。

8) 保護管理者によるレビュー

保護管理者は報告を受けた「ＰＭＳ教育計画書」、「ＰＭＳ教育実施記録」に問題がある場合は、教育内容の追加や改善について教育責任者に指示する。

保護管理者の指示について、教育責任者は、臨時の教育を計画するか、次期教育計画に反映する等の対応を行う。

9) 教育の記録の保持に関する責任及び権限

教育の計画や、実施記録等の記録の保持に関する責任者は、教育責任者とする。教育関係の記録は最低３年間保管する。

A.3.5 文書化した情報

A.3.5.1 文書化した情報の範囲

(1) 健康推進機構は、次のＰＭＳの基本となる要素を書面で記述する。

a) 内部向け個人情報保護方針

b) 外部向け個人情報保護方針

c) 内部規程

d) 内部規程に定める手順上で使用する様式

e) 計画書

f) この規格が要求する記録及び健康推進機構がＰＭＳを実施する上で必要と判断した記録

A.3.5.2 文書化した情報（記録を除く。）の管理

(1) 健康推進機構は、この規格が要求するすべての文書化した情報（記録を除く。）を管理する手順を

確立し、実施し、かつ、維持する。

(2) 文書管理の手順には、次の事項を含める。

a) 文書化した情報（記録を除く。）の発行及び改訂に関すること

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

(3) 健康推進機構は、ＰＭＳ文書を「ＰＭＳ文書管理台帳」にて管理し、文書管理台帳には、以下の項目を含める。

－ 文書管理番号
－ 文書名
－ 版数
－ 発行日（もしくは改訂日）
－ 文書管理者
－ 保管場所
－ 保管期間
－ 廃棄方法

(4) ＰＭＳ文書の識別、管理等については、以下のとおりとする。

1) 文書の識別方法

・健康推進機構は、文書管理番号、文書名、版数によってＰＭＳの文書を管理する。

文書管理番号

規程：健康推進機構のＰＭＳの規定を記述した上位文書

ＰＭＫ－ｎｎｎ：ｎｎｎは文書単位に独自番号を付す。

手順：規程類から参照される下位文書で、詳細なあるいは、具体的な手順を定める

ＰＭＴ－ｎｎｎ：ｎｎｎは文書単位に独自番号を付す。

様式：内部規程に定める手順上で使用する様式

ＰＭＹ－ｎｎｎ：ｎｎｎは様式単位に独自番号を付す。

文書名

規程名又は手順書名及び様式名

版数

第Ｎ．ｎ版（新規発行時は１．０版とし、以降改訂ごとにｎを０．１ずつアップして旧版と混在しないよう識別する。JIS 規格等が改正され、健康推進機構が作成した規程類の大幅変更が必要な場合は、Ｎをアップする場合もある）

尚、旧版を参照するために保管する場合は、表紙に「旧版」と明記し識別する。

2) 文書の発行、改訂

・文書の発行、改訂は「ＰＭＳ文書管理台帳」に記載されている文書管理者が行い、保護管理者の承認を得る。

「ＰＭＳ文書管理台帳」の発行日（もしくは改訂日）は、保護管理者の承認日を記載する。

・文書を改訂した場合は、版数をアップし、規程・手順の改訂履歴の“改訂内容”欄に、当該版数に対応した文書の改訂内容を記入し、関連付けを明確にする。

3） 文書の配布又は公表

・ＰＭＳ文書の規程・手順は、保護管理者が原本を保管管理し、写しを理事長、保護管理者、監査責任者、監査員、教育責任者、部門管理担当者、部門長に配布する。
改訂版を配布する際は、旧版を回収し、再利用できない方法により廃棄する。

・ＰＭＳ文書の規程・手順は、ＰＤＦ化等の改ざん防止対策を行い、社内イントラネットで公表し、必要なときに、必要な文書を容易に参照できる措置をとる。様式は、原本を、共有フォルダに複写し、共有エリアの様式を利用可能とする。改訂の際は、改訂内容を社内掲示板等に公表する。また、大幅な改訂が行われた場合は、改訂内容について教育等で従業者に周知する。

A.3.5.3　文書化した情報のうち記録の管理

(1) 健康推進機構は、ＰＭＳ及びこの規格の要求事項への適合を実証するために必要な記録として、次の事項を含む記録を作成し、かつ、維持する。

(2) 健康推進機構は、記録の管理についての手順を確立し、実施し、かつ維持する。

a） 個人情報の特定に関する記録
b） 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
c） 個人情報保護リスクの認識、分析及び対策に関する記録
d） 計画書
e） 利用目的の特定に関する記録
f） 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
g） 教育などの実施記録
h） 苦情及び相談への対応記録
i） 運用の確認記録
j） 内部監査報告書
k） 是正処置の記録
l） マネジメントレビューの記録

(3) 健康推進機構で必要な記録は、上記で示すJIS規格で必要とする記録と、安全管理措置で実施した記録とするが、ＰＭＳの記録類は「ＰＭＳ記録管理台帳」で管理する。

なお、「ＰＭＳ記録管理台帳」には、次の項目を含める。

－ 記録名
－ 作成者
－ 作成日
－ 保管場所（保管方法）。
－ 保管期間
－ 廃棄方法
－ 個人情報有無（個人情報を含むか否かの区分）

「ＰＭＳ記録管理台帳」は、記録を作成した部門単位に管理する。

(4) 記録は、紙媒体である必要はないが、電磁媒体に保管する場合は、改ざんや上書きによる消失、誤

消去等のリスクから保護するための措置を講じる。紙媒体の記録は、漏えいや改ざん、不適切な使用を防止するために、閲覧時以外は施錠キャビネットに保管するなどの措置を講じる。

A.3.6　苦情及び相談への対応

(1) 健康推進機構は、個人情報の取扱い及びＰＭＳに関して、本人からの苦情及び相談を受け付け、適切かつ迅速な対応を行う手順を確立し、かつ、維持する。

(2) 健康推進機構は、上記の目的を達成するために必要な体制の整備を行う。

1) 苦情及び相談の窓口

健康推進機構の苦情及び相談の窓口は、苦情相談窓口とする。苦情及び相談の窓口については、健康推進機構ホームページ「個人情報保護方針」で公表する。

2) 苦情及び相談の対応手順

① 電話、電子メール等で苦情及び相談を受け付けた場合は、「苦情相談対応記録」に、苦情内容と受付日を記録する。

② 苦情相談窓口は、苦情及び相談の内容の確認を行い、個人情報の取扱いに関する苦情、又はＰＭＳに関する苦情かによって、対応部署に調査を依頼する。

③ 苦情相談窓口は、苦情内容が健康推進機構の信頼性の喪失や、取引機会の喪失につながる恐れ又は健康推進機構のＰＭＳに問題があると判断した場合、理事長に報告するとともに、是正処置の対象とする。

④ 調査を依頼された部門は、速やかに調査を行い、対象となる資料がある場合は資料を添付し、苦情相談窓口に、調査結果を回答する。

⑤ 調査結果に基づき、苦情相談窓口は、「苦情相談対応記録」の回答欄に記載し、回答内容について保護管理者が承認し、理事長に報告する。保護管理者が重大な苦情及び相談と判断した場合は、理事長の承認を得る。

⑥ 苦情相談窓口は、「苦情相談回答書」にて、苦情及び相談者本人に対して回答を行う。また、「苦情相談対応記録」の回答日を記載する。なお、受付から回答までは、７営業日を目安とする。

3) 是正処置が必要な場合

苦情相談窓口が「是正処置報告書」を起票し、是正処置及び予防処置の手順に従って対応する。原因が健康推進機構のＰＭＳの不備による場合は、リスクアセスメントにフィードバックし、リスクアセスメント結果から適切な対策を行う。

A.3.7　パフォーマンス評価

A.3.7.1　運用の確認

(1) 健康推進機構は、ＰＭＳが適切に運用されていることが健康推進機構の各部門及び階層において定期的に、及び適宜に確認されるための手順を確立し、実施し、かつ、維持する。

(2) 各部門及び各階層の管理者は、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し、不適合が確認された場合は、その是正処置を行う。

(3) 保護管理者は、理事長によるＰＭＳの見直しに資するため、定期的に、及び適宜に理事長にその状

況を報告する。

(4) 健康推進機構は、次の事項について毎月１回、定期的に運用の確認を行う。運用の確認は、各部門長及び情報システム管理者が行う。確認の結果については「運用確認記録」に記録する。

1) 最終退出時の社内点検（施錠確認等）

2) 入退館（室）の記録の確認

3) アクセスログの定期的な確認

A.3.7.2 内部監査

(1) 健康推進機構は、ＰＭＳの JIS 規格への適合状況及びＰＭＳの運用状況を定期的（少なくとも年１回）、適宜に監査する。

(2) 健康推進機構は、監査の計画及び実施、結果の報告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を確立し、実施し、かつ、維持する。

(3) 個人情報保護監査責任者は、監査員に、自己の所属する部署の内部監査をさせてはならない。

(4) 内部監査の実施等については、以下のとおりとする。

1) 監査の適用範囲

健康推進機構の全部門を監査の対象とする。個人情報の取扱いが無いと判断している部門であっても、本当に個人情報の取扱いがないか、従業者の個人情報の取扱状況はどうか、ＰＭＳが浸透しているか等の監査を行う。

2) 監査計画書の作成

監査責任者は、毎年期首に「ＰＭＳ内部監査計画書」を作成し、理事長の承認を得る。

内部監査計画書には、JIS との適合性監査と、各部門、管理者毎の運用状況の監査の実施予定を明確にする。標準的な実施時期は、以下の通りとする。

JIS との適合性監査：１１月

運用状況の監査　　：１～２月

上記の定期監査値は別に、必要に応じて随時実施する。

なお、JIS 規格との適合性監査は、ＰＭＳ事務局を対象として行う。なお、内部規程等の改正がなければ毎年行う必要はないが、事業環境の変化、法令等の制定改廃、リスク状況の変化などにより、内部規程の改正漏れが生じていないか監査する。

3) 監査実施準備

監査責任者は、「ＰＭＳ内部監査計画書」で計画した監査実施の 1 ヶ月前に、「ＰＭＳ個別内部監査計画書」を作成して、関係部署に通知する。また、「ＰＭＳ個別内部監査計画書」には、監査の実施日、時間、担当監査員、重点監査項目、監査適用条項等を明確にする。

監査責任者は、監査員を部署ごとに割り振るにあたっては、監査員が、自ら所属する部門の監査を実施しないように配慮して編成を行う。

監査は、次の内部監査チェックリストを使用して行うが、監査実施前に監査責任者は、監査チェックリストの監査項目に過不足がないか事前確認を行い、過不足がある場合は、見直しを実施する。

JIS との適合性監査：「ＰＭＳ内部監査チェックリスト(適合性監査)」

運用状況監査　　:「ＰＭＳ内部監査チェックリスト(運用状況)」

運用状況の内部監査チェックリストには A.3.3.3 リスクアセスメント及びリスク対策により講じることとしたリスク対策が実施されているか、残留リスクが顕在化していないか等のチェック項目を含める。

4) 監査の実施

監査員は、「ＰＭＳ個別内部監査計画書」、「ＰＭＳ内部監査チェックリスト」に基づいて、対象部門の監査を実施する。監査にあたっては、「ＰＭＳ内部監査チェックリスト」のチェック項目ごとに、確認した客観的な証拠を明確に記述する。

監査員は、部署ごとの監査終了後に「ＰＭＳ内部監査実施報告書」を作成し、監査責任者に報告する。不適合があれば、1件1葉で「是正処置報告書」を作成し「ＰＭＳ内部監査実施報告書」に添付する。

監査責任者は、「ＰＭＳ内部監査実施報告書」と「是正処置報告書」を理事長に提出し承認を受ける。

理事長の承認を得た「ＰＭＳ内部監査実施報告書」、「是正処置報告書」は、写しを取り、被監査部門に原本を通知する。写しは、監査責任者が保管する。

また、監査責任者は全部門の監査が終了した後、速やかに「ＰＭＳ内部監査総括表」に内部監査状況をまとめて記入し理事長に報告する。この「ＰＭＳ内部監査総括表」をマネジメントレビューのインプットとする。

5) 是正処置の実施

被監査部門は、「是正処置報告書」による不適合があれば、是正措置を実施する。是正処置は、A.3.8 是正処置の手順に従う。

是正処置の実施結果については、監査員がその適切性を確認する。

是正処置が終了した時点での有効性についての確認は、監査責任者行い、理事長が承認する。

是正処置の完了した「是正処置報告書」の原本は、監査責任者が回収し、他の監査の記録とともに保管する。

6) 責任及び権限

監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する責任者は、監査責任者とする。監査関係の記録は、最低３年間保管する。

A.3.7.3 マネジメントレビュー

(1) 理事長は、個人情報の適切な保護を維持するために、少なくとも年 1 回、適宜にＰＭＳを見直す。マネジメントレビューにおいては、次の事項を考慮する。

a) 監査及びＰＭＳの運用状況に関する報告

b) 苦情を含む外部からの意見

c) 前回までの見直し結果に対するフォローアップ

d) 個人情報の取扱いに関する法令、国の定める指針その他の規範の改正状況

e) 社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化

f) 組織の事業領域の変化

g) 内外から寄せられた改善のための提案

(2) マネジメントレビューの実施等については、以下のとおりとする。

1) 健康推進機構は、毎年期末（３月)に定期的にマネジメントレビューを実施する。経営環境の大幅な変化、法令等の改正、事業領域の変化により取り扱う個人情報が変化した場合などに、必要に応じて随時マネジメントレビューを開催する。マネジメントレビューは「マネジメントレビュー実施記録」に記録し、最低３年間保管する。

2) 「マネジメントレビュー実施記録」には、理事長の指示項目欄を設け、次回のマネジメントレビュー時に理事長の指示に対する対応状況として c)項で報告する。

3) マネジメントレビューのインプットには a)～g)を含めるが、毎回全てを見直しのインプットとする必要はない。当該年度で該当しない事項に関しては“該当なし”と明確に記述する。

A.3.8 是正処置

(1) 健康推進機構は、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を確立し、実施し、かつ、維持する。その手順には、次の事項を含める。

a) 不適合の内容を確認する。

b) 不適合の原因を特定し、是正処置を立案する。

c) 期限を定め、立案された処置を実施する。

d) 実施された是正処置の結果を記録する。

e) 実施された是正処置の有効性をレビューする。

(2) 是正措置の対象及び手順等については、以下のとおりとする。

1) 是正処置の対象

健康推進機構は、次の事象により発見された不適合に対して、是正処置を実施する。

- 外部機関による審査
- リスクなどの認識、分析及び対策
- 緊急事態の発生
- 苦情
- 運用の確認
- 監査

2) 是正処置の実施手順

発見された不適合を改善するための是正処置は以下の手順で実施する。

① 上記の不適合を発見された部署が一件一葉で「是正処置報告書」を起票し、保護管理者又は監査責任者が不適合の内容を確認し理事長に報告し、承認を得る。軽微な不適合の場合は、保護管理者又は監査責任者が承認する。

② 理事長あるいは保護管理者又は監査責任者の承認を得た「是正処置報告書」は不適合を発見された部署に返却する。不適合を発見された部署は不適合の原因を特定し、是正処置を立案する。不適合に対する原因分析は、不適合の原因に対する対策が是正処置であることを認識して、現象を記述するのではなく根本的な原因を追究した結果を記述する。

原因に対する対策を立案し、対応予定期限を明確に記述し、理事長（軽微な場合は保護管理者あるいは監査責任者）の承認を得る。

承認者は、立案した是正処置が適切でないと判断した場合は、差し戻し是正処置計画の見直しを要求する。

③ 不適合を発見された部署は、立案した是正処置を対応予定期限までに実施し、「是正処置報告書」に実施した内容と、実施者、完了日等を記述する。是正処置実施に伴って作成した記録類（教育の記録、運用の確認の記録等）は当該の「是正処置報告書」と一緒に保管する。

④ 実施した是正処置の有効性をレビューする。有効性のレビューは軽微な場合は、運用の確認に含めて各部署で実施し、それ以外は不適合が改善されているかどうかを、フォローアップ監査を実施して確認する。フォローアップ監査は、監査責任者もしくは，監査責任者に委任された監査員が実施する。

⑤ 有効性のレビューの結果を、運用の確認者、もしくは監査者が記入し、個人情報保護管理者に報告する。個人情報保護管理者は、再発が見られ、有効性がないと判断した場合、原因分析及び是正処置の立案から再度のやり直しを命じる。また、必要に応じて、リスクアセスメントにフィードバックし、リスクアセスメント結果のリスク対策を、規程類に盛り込む。保護管理者は、レビュー結果を理事長に報告し承認を得る。

⑥ 監査に関する「是正処置報告書」は監査責任者が保管管理する。それ以外の不適合に関する「是正処置報告書」は保護管理者が保管する。

附　則

1　この規程は、令和３年４月１日から施行する。

2　個人情報保護管理規程（平成１７年４月１日制定）は廃止する。

3　この規程は、令和４年８月９日から施行する。