# 個人情報保護規程

第３．１版

発行日：2025年４月１日

| 承認日 | 作成日 |
|---|---|
| 2025年３月13日 | 2025年3月11日 |
| 承認者 | 作成者 |
| 間中 英夫 | 渡邉　一夫 |

改版履歴

| 版数 | 発行日 | 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 |
| 3.0 | 2024.4.1 | 日本情報経済社会推進協会（JIPDEC）公表の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・運用指針及び一般財団法人医療情報システム開発センター（MEDIS）公表の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 版に基づき全面改訂 |
| 3.1 | 2025.4.1 | 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および内部監査での指摘、その他修正に伴う改訂 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# 目次

## 本規程文書の目的及び適用範囲

本規程は、業務上取扱う個人情報の適切な使用と保護のため、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。）日本情報経済社会推進協会が策定した「**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**」（以下、ＰＭＳ運用指針という。）、日本産業規格 **JISQ15001**「個人情報保護マネジメントシステムー要求事項」（以下、JISQ15001 という。）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、実施し、維持し、及び改善するために必要な基本的事項を定めることを目的とする。

本規程の適用範囲は、健康推進機構が自らの事業の用に供している個人情報に関する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、改善するため業務上取扱う全ての個人情報として、従業者（理事長、理事、局長、役員、職員、派遣職員、パートタイマー、アルバイト、実習生、ボランティア等）及び個人情報の保護対象（採用情報も含む）を対象とする。

## J.0 用語および定義

・規程で用いる主な用語及び定義は次の通りとする。

(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) 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。

(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。

(4) 本人

個人情報によって識別される特定の個人。

(5) 事業者

事業を営む法人その他団体又は個人。

(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。）

(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。）

(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。

(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。

(10) リスク

目的に対する不確かさへの影響。

(11) 残留リスク

リスク対応後に残っているリスク。

(12) リスク対応

リスクを修正するプロセス。

(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。

(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。

(15) 管理策

リスクを修正する対策。

(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。

(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。

(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。

(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。）

(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。

## J.1 組織の状況

### J.1.1 組織及びその状況の理解（JISQ150014.1）

(1) 健康推進機構は、個人情報を取り扱う事業に関して、個人情報保護の目的を明確にし、構築・維持している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する。

(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を維持するうえで、外内部からの課題を整理し、個人情報保護の目的と「**課題一覧表**」にまとめ、理事長の承認を得る。

### J.1.2 利害関係者のニーズ及び期待の理解(JISQ150014.2)

(1) 健康推進機構は、個人情報保護マネジメントシステムを運用するにあたり、次の事項を特定する。

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

(2) 個人情報保護管理者は、本項(1)の a)、b)について検討し、「**課題一覧表**」にまとめ、理事長の承認を得る。

### J.1.3 法令、国が定める指針その他の規範（JISQ15001 附属書 A.3.3.2）

(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、関連内規及び「個人情報関連法規一覧表」を可及的速やかにその改廃内容を必要に応じて更新する。

(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関する法律施行令」
3) 「個人情報の保護に関する法律に関する法律施行規則」
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（通則編）」
5) 「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）」
6) 「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）」
7) 「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）」
8) 「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」
9) 「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」
10) 「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）」
11) 「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）」
12) 「診療情報の提供等に関する指針」

### (6) J.1.4　　個人情報保護マネジメントシステムの適用範囲（JISQ150014.3）

(1) 健康推進機構は、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して定め、その旨を文書化する。

### J.1.5 個人情報保護マネジメントシステム（JISQ150014.4）

(1) 健康推進機構は、ＰＭＳ運用指針に従って、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、継続的に改善する。

(2) 具体的な手順は、本規程 J.2～J.11 に定める。

## 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（JISQ150015.1）

(1) 理事長は、次の事項について統率し、その結果について責任を持つものとする。

a) 健康推進機構の戦略的な方向性と両立した、個人情報保護方針及び個人情報保護目的を確立する

b) 個人情報保護マネジメントシステムの要求事項を健康推進機構の業務手順に適切に組み入れる

c) 個人情報保護マネジメントシステムに必要な資源を確保する

d) 有効な個人情報保護マネジメント及び個人情報保護マネジメントシステム要求事項への適合の重要性を利害関係者に周知する
e) 個人情報保護マネジメントシステムを適切に運用できるようにする
f) 個人情報保護マネジメントシステムが計画通りに実施できるように、従業者を指揮･支援する
g) 継続的改善を促進する
h) その他の関連する管理者がその職務領域において、統率力を発揮できるよう、その管理者に割り当てられた役割をサポートする

### J.2.2 個人情報保護方針(JISQ150015.2.1、5.2.2、附属書 A.3.2.1、A.3.2.2)

(1) 理事長は、個人情報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) 事業の目的に対して適切であること
b) J.3.2 で定めた個人情報保護目的を含むか、又は個人情報保護目的の設定のための枠組みを示すこと
c) 個人情報保護に関連して適用される要求事項を実施すること
d) 個人情報保護マネジメントシステムの継続的改善を実施すること
(2) 個人情報保護方針を文書化した情報には、次の事項を含める。
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その他の規範の遵守
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事項
d) 苦情及び相談への対応に関する事項
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事項
f) 理事長の氏名
g) 制定年月日及び最終改正年月日
h) 個人情報保護方針の内容についての問合せ先
(3) 理事長は、個人情報保護方針を文書化し、会議や定期的な教育等で従業者に周知させるとともに、必要に応じて社外の利害関係者及び一般の人が容易に入手可能な措置（ウェブページへの掲載及び受付や診察室での掲示等）を講じる。

### J.2.3 組織

### J.2.3.1 組織の役割、責任及び権限（JISQ150015.3）

(1) 理事長は、個人情報保護に関連する役割に対して、責任及び権限を従業者へ割り当てるとともに、その結果を、定期教育などを利用して利害関係者に周知するものとする。

(2) 責任及び権限を、次の事項を実施するために割り当てること。
   a) 個人情報保護マネジメントシステムを、本指針の要求事項に適合させる。
   b) 個人情報保護マネジメントシステムの運用の成果を理事長に報告させる。
(3) 理事長は(2)を実施するため、個人情報保護管理者及び個人情報保護監査責任者を指名し、ＰＭＳを実施、監査させる。
   理事長の承認権限に関しては、個人情報保護方針の策定・改定以外は、しかるべき職務権限を持つ者に委譲することができる。権限委譲する場合は、健康推進機構が別途定める手順による。
(4) 個人情報保護管理者、個人情報保護監査責任者は与えられた役割を行うために、必要な担当者を任命することができる。
(5) 電子カルテ等の情報システムを導入している場合は、システム内部管理者を内部から選任する。

### J.2.3.2 個人情報保護管理者、個人情報保護監査責任者及びその他の役割

(JISQ15001 附属書 A.3.3.4)

(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（JIS Q 15001:2023)』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。 |
| 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。 |
| 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。 |

### J.2.4 管理目的及び管理策（一般）（JISQ15001 附属書 A.3.1.1）

(1) J.1 から J.11 の管理策及びその結果について、理事長又は理事長によって権限が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ものとする。

(2) 承認者（決裁権限者）は、承認内容に照らし合わせて、適切に定める。

(3) 本規程では、J.1 から J.11 の管理策及びその結果の承認者、承認手順は、各項において定める。

## J.3 計画

### J.3.1 計画

### J.3.1.1 個人情報の特定（JISQ15001 附属書 A.3.3.1）

(1) 健康推進機構は、健康推進機構が自らの事業の用に供する全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。

(2) 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。

(3) 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。

(4) 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。

(5) 「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（概数でも可）
- 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」の内容において取扱いの変更が生じた場合は、「個人情報管理台帳」に“修正案”を記載のうえ、保護管理者の承認を得て「個人情報管理台帳」を“更新”する。また、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。

(6) 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、「個人情報取扱申請書」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。

### J.3.1.2 リスク及び機会に対処する活動（JISQ150016.1.1）

(1) 健康推進機構は、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、次の事項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行うものとする。

a)健康推進機構が意図した成果を達成できるようなマネジメントシステムの策定

b)望ましくない影響の防止

c)個人情報保護マネジメントシステムの継続的な改善

(2) 健康推進機構は、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、次の事項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行うものとする。

d)リスクに対する対策の内容

e)“d)”の対策を個人情報保護マネジメントシステムの手順に含めて実施する方法

f)“d)”の対策の評価

### J.3.1.3 個人情報保護リスクアセスメント（6.1.2、附属書A.3.3.3）

(1) 健康推進機構は、個人情報に関するリスクについて、次の事項を踏まえて、個人情報保護リスクアセスメント（リスクを特定、分析及び評価）をするために以下のa)～d)の手順を本規程J.3.1.4に定め、かつ実施する。

a) 次の観点を、個人情報保護のリスク基準とする。

1) 本規程に定める事項

2) 法令及び国が定める指針その他の規範に関する事項

3) 個人情報の漏えい、滅失又はき損等に関する事項

b) 個人情報保護リスクアセスメントを行う際に、繰り返し実施した個人情報保護リスクアセスメントに、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確認し、必要に応じて手順を見直す。

c) 個人情報保護リスクを特定する

1) 健康推進機構は、事業毎に、個人情報の取扱いを特定する

2) 個人情報の取得、保管、利用及び消去等に至る各局面において、適正な保護措置を講じない場合に想定されるリスクを特定する

3) 上記で特定したリスクのリスク所有者を特定する

d) 個人情報保護リスクを分析・評価する

1) “c)”で特定したリスクと、“a)”のリスク基準とを比較する

2) リスク対応の優先順位を明らかにする

(2) 個人情報を特定する手順は本規程J.3.1.1に定める。

### J.3.1.4 個人情報保護リスク対応（6.1.3、附属書A.3.3.3）

(1) リスクの認識、リスクアセスメント、リスク対策は、以下の要領で行い、「**リスクアセスメント表**」に記述し、個人情報保護管理者が承認した後に、「**リスクアセスメント表**」のリスク対応策の内容に、人･物･金等の経営資源の観点から理事長の承認を得る。

a) 個人情報の業務の流れの類型化を図る

「個人情報管理台帳」に特定した個人情報の取扱いごとに以下の手順でリスクアセ

スメントを行い、検討したリスク対策を「**リスクアセスメント表**」にまとめる。この際、業務の流れ（ライフサイクル局面）が同じ個人情報についてグループ化しリスク分析を集約することが可能である。

b) ライフサイクル局面ごとのリスクを記述する

個人情報のライフサイクル（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）それぞれについて考えられるリスクを想定リスクとして「**リスクアセスメント表**」に記述する。

なお、想定リスクには、本規程 J.3.1.3(1)の(a)1)、2)の事項に違反するリスク及び(a)3)の事項による発生リスクを含めるとものとする。

特定したリスクの所有者は個人情報保護管理者または個人情報保護管理者が指定した部門管理責任者とする。

c) リスクのレベルを判定する。

1) 想定リスクの発生可能性を“高”、“中”、“低”に分類する。

2) 想定リスクによる影響度合いを“大”、“中”、“小”に分類する。

3) 下表を用いてリスクレベルを“高”、“中”、“低”に分類し、「**リスクアセスメント表**」に記入する。

| リスクレベル | | 発生可能性 | | |
|---|---|---|---|---|
| | | 高 | 中 | 低 |
| 影響 | 大 | 高 | 高 | 中 |
| | 中 | 高 | 中 | 低 |
| | 小 | 中 | 中 | 低 |

d) リスク対策を記述する

1) 想定リスクごとに対策を「**リスクアセスメント表**」に記入する。

なお、対策を立案する場合には、本規程 J.3.1.2(1)の a)～c)の内容を加味するものとする。

2) リスクの対策は、リスクレベルに応じて実施負荷などを踏まえ決定する。

3) リスクレベルは同時に、リスク対策の優先度とする。

e) 関連する規程類の記入

講じるとしたリスクの対策を定めた規程文書名、項番を「**リスクアセスメント表**」に記入する

f) 残留リスクの記述

1) 対策後においても人・物・金等の制約でリスクを完全には回避できない未対応部分を、残留リスクとして「**リスクアセスメント表**」に記述する。

2) 記述した残留リスクは、定期的にその脅威や脆弱性が増加していないかを定期的に確認する手段も検討し、記録する。

(2) 「**リスクアセスメント表**」の更新

① 利用目的変更・取扱い方法変更の場合

a) 部門管理責任者は、変更する前の「**リスクアセスメント表**」を参考に、当該部門の取り扱う個人情報の想定リスク、リスク対策、リスク対策の規程、残留リスク等のリスク分析の見直しを行う。

b) 個人情報保護管理者の承認の後に、リスク対策に理事長の承認を受ける。

② 個人情報を削除する場合

a) 「**リスクアセスメント表**」から当該個人情報を削除する。この際、削除履歴が残るようにしておく。

b) 個人情報保護管理者の承認の後に理事長に報告する。

(3)「**リスクアセスメント表**」の見直し

「**リスクアセスメント表**」は、毎年４月に、部門管理責任者が見直しを行い、個人情報保護管理者の承認の後に、リスク対策に理事長の承認を受ける。

随時見直しは部門管理責任者が新業務の追加や既存業務の変更、外部環境の変化などからリスクの見直しを実施することを決め、実施し、個人情報保護管理者の承認の後に、リスク対策に理事長の承認を受ける。

### 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（6.2）

(1) 理事長は個人情報保護目的を達成するために、教育、内部監査、安全管理計画（情報セキュリティ対策）、委託先の監督、マネジメントレビューの実施などを、以下のa)～e)含めた計画を策定することを、個人情報保護管理者、個人情報保護監査責任者等に指示する。

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

(2) 具体的な計画手順は、本規程J.3.3（計画策定（JISQ15001 附属書A.3.3.6））、J.6.2（内部監査（JISQ15001 9.2、附属書A.3.7.2））、J.6.3（マネジメントレビュー（JISQ15001 9.3、附属書A.3.7.3））、J.9.4（委託先の監督（JISQ15001附属書A.3.4.3.4））などに定める。

### J.3.3 計画策定（JISQ15001附属書A.3.3.6）

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。

## J.4 支援（表題）

### J.4.1 資源（7.1）

(1) 健康推進機構は、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、利害関係者へ提供するものとする。

### J.4.2 力量（7.2）

(1) 健康推進機構は、個人情報保護マネジメントシステムを適切に運用するため、次の事項を行う。

a) 健康推進機構の個人情報保護に影響を与える業務をその管理下で遂行する者に対して、個人情報保護の観点から、従業者に必要とされる能力を決定する

b) “a)”の者に対して、“a)”で決定した能力及びJ.4.3を充足するための処置を行い、必要な能力を備えることを確実にする

c) “b)”を実施した結果、必要な能力が備わっていない場合は、必要な能力を身につけるための処置をとるとともに、とった処置の有効性を評価する

d) “a)～c)”を実施した記録を保持する

### J.4.3 認識（7.3）

(1) 健康推進機構は、すべての従業者（退職者を除く）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。

### J.4.4 コミュニケーション

#### J.4.4.1 コミュニケーション(7.4)

(1) 健康推進機構は、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、次の事項を考慮して、内外の利害関係者と意思疎通や情報共有を行うこととする。

a) コミュニケーションの内容（伝達する内容）
b) コミュニケーションの実施時期
c) コミュニケーションの対象者
d) コミュニケーションの実施者

e) コミュニケーションの実施手順
f) コミュニケーションの実施方法

### J.4.4.2 緊急事態への準備（JISQ15001 附属書 A.3.3.7）

(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、法令等の定めに基づき、次の事項を含む対応手順を確立し、かつ、維持するものとする。
a) 漏えい、滅失又はき損が発生した個人情報の内容を本人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などの観点から、事案の内容などに応じて、可能な限り事実関係、発生原因及び対応策を、速やかに公表すること。
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
健康推進機構では緊急事態とは以下の場合を指すものとする。
① 個人情報の漏えい、紛失、滅失又はき損の発生
② 個人情報の改ざん、正確性の未確保状態の発生
③ 不正・不適正取得の発生
④ 目的外利用・提供の発生（適用除外事項に該当する場合を除く）
⑤ 不正利用の発生
⑥ 開示などの求め等の拒否（適用除外事項に該当する場合を除く）
⑦ 上記①～⑥の恐れ
⑧ 火災や地震等により、個人情報を取り扱う業務に重大な支障をきたすと思われる場合
⑨ システム上もしくはネットワーク上に重大な障害が発生し、個人情報の適正管理に支障をきたすと、システム管理責任者が判断した場合
⑩ 個人情報に関連する脅迫行為が行われた場合
(5) 緊急時への準備及び処置要領
① 緊急事態の特定のため、個人情報のリスクにより本人への影響度に応じた対応のためのレベル区分を設定する。
② 緊急事態発生時の初動対応のための報告及び対応体制の確立
③ 緊急事態の発生（発生確認）時の初期における事態の拡大防止等のための一次対応
④ 緊急事態の細部状況の把握、再発防止の及び関係者への謝罪、外部への公表をおこなう。

(6) 基本的な対応基準（レベル分け）

個人情報保護管理者は漏洩、滅失または毀損が発生した個人情報の重要度により以下のレベル区分とする。

| レベル | 影響度(事例) |
|---|---|
| A(低) | 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<br>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。 |
| B(中) | 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。 |
| C(高) | レベルＢで「緊急事態」に特定され、個人情報保護規程 J.4.4.2 に該当する事故等が発生した場合。 |

(7) 緊急事態発生時の初動対応

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。

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。

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。

(8) 緊急時における対応手順

緊急時における一次対応は、被害状況の把握及び被害の拡大防止、二次被害の防止の観点により、経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し以下の手順で行う。

① 個人情報保護管理者は、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 緊急事態の類型による初期対応

a) 警察への通知（盗難、強盗などの事件の場合）

b) 対象となった個人情報、被害規模、範囲の特定（全ての場合）

c) システム停止等の応急措置（システム障害の場合）

d) 受託業務の場合は委託元への報告と協議し、委託元の指示に従う。

e) 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、関係審査機関（以下 1）～9)の場合)、委員会（以下 1）～8)の場合）及び本人（以下 1）～8)の場合）への速やかな報告(5 日以内)を行う。

1) 要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態

2)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個人データの漏えい等が発生し、又は発生したおそれがある事態

3)不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、

又は発生したおそれがある事態

4)個人データに係る本人の数が 1000 人を超える漏えい等が発生し、又は発生したおそれがある事態

5)次に掲げる特定個人情報（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

(ア)情報提供ネットワークシステム及びこれに接続された電子計算機に記録されたマイナンバー

(イ)個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理されるマイナンバー

(ウ)行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番号関係事務を処理するために使用する情報システムにおいて管理されるマイナンバー

6)次に掲げる事態

(ア)不正の目的をもって行われたおそれがあるマイナンバーの漏えい等が発生し、又は発生したおそれがある事態

(イ)不正の目的をもって、マイナンバーが利用され、又は利用されたおそれがある事態

(ウ)不正の目的をもって、マイナンバーが提供され、又は提供されたおそれがある事態

7)個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

8)次に掲げるマイナンバーに係る本人の数が 100 人を超える事態

(ア)漏えい等が発生し、又は発生したおそれがあるマイナンバー

(イ)番号法第９条の規定に反して利用され、又は利用されたおそれがある個人番号を含むマイナンバー

(ウ)番号法第 19 条の規定に反して提供され、又は提供されたおそれがある特定個人情報

9)P マーク付与機関が P マーク審査基準における重大な違反の恐れがあると認めた事態

f)受託業務以外で、上記 e)の 1)～8)及び一般財団法人日本情報経済社会推進協会（JIPDEC）が P マーク審査基準における事故等（上記(4)①～⑦）の発生及び重

大な違反のおそれがあると認めた事態に、関係機関への速やかな報告（発覚した日から起算して 5 日以内）を行う。

③ 危機管理対策本部の開催

a) 危機管理対策本部にて対応方針決定する。

b) 対応策を実施し、その記録を「**事故報告**」にて記録する。

④ 本人への通知（健康推進機構が直接取得した個人情報や提供を受けた個人情報の場合（委託先で事故が発生した場合も含む））

a) 特定された本人に対し電話やメール等で連絡を行い、事実関係及び、具体的な対応策を説明し、了承を得る。

b) 本人への連絡事項には少なくとも以下の事項を含める。

1) 事故概要

2) 個人データの項目

3) 事故原因

4) 二次被害の有無及びその内容

5) その他参考となる事項

c) 了承を得られない場合には、危機管理対策本部にて改めて対応を協議の上、決定事項に基づいて本人への対応を行う。

d) 連絡がつかない場合、及び本人特定ができない場合は、ウェブページでの公表など内容を本人が容易に知りうる状態に置く。

⑤ 本人への通知（受託業務などで預かっている個人情報の場合（再委託先で事故が発生した場合も含む））

a) 委託元に事故内容の連絡を行い、本人への通知も委託元の指示に従う。

b) 本人への連絡事項には少なくとも以下の事項を含める。

1)事故概要

2)個人データの項目

3)事故原因

4)二次被害の有無及びその内容

5)その他参考となる事項

⑥ 公表

a) 危機管理対策本部において公表が必要と判断した場合には、健康推進機構ウェブページを通じて事実関係及び、発生原因、対応状況、再発防止策などを公表する。

b) 影響範囲が広範囲かつ深刻な場合は、マスコミへの公表を行う。

c) 公表を行う場合は、マスコミ等外部に対する問合せ窓口を設置する。

⑦ 関係機関への確定報告

危機管理対策本部における決定に基づき、

②の e)1)～8)に該当する場合またはレベルＢに分類される事故について、個人情報保護委員会に、又同様に本項(4)①～⑦の事態に該当する場合には健康推進機構のＰマーク審査機関に、それぞれ確定報告を行う。（原則 30 日以内、不正の目的をもって行われた恐れがある事故等の場合には 60 日以内）報告内容には以下の内容を含める。

1)事故概要
2)個人データの項目
3)個人データに係る本人の数
4)事故原因
5)二次被害の有無及びその内容
6)本人への対応の実施状況
7)公表の実施状況
8)再発防止のための措置
9)その他参考となる事項

(9) 関係機関より、対応について指示のある場合は、すみやかにそれに従う。

(10)認定個人情報保護団体に所属している場合、その連絡は各認定個人情報保護団体の指示に従う。

(11)緊急事態発生時における作業記録

個人情報保護管理者は、事後の係争への対処及び業務改善のため、緊急事態発生時における、対応内容を「**事故報告**」にまとめて、その記録を保管する。

① 外部からの問い合わせ、クレームの内容など
② 対外連絡、報告、協議に関する事項
③ 社内における連絡、報告、協議に関する事項

(12)緊急事態への恒久的対応

緊急事態における一次対応が収束し、被害の拡大がないと理事長が判断した場合には、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。

## J.4.5 ＰＭＳ文書

### J.4.5.1 文書化した情報（一般）（JISQ150017.5.1、附属書 A.3.5.1）

(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) 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）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

### J.4.5.2 文書化した情報の管理（JISQ150017.5.3）

(1) 健康推進機構は、個人情報保護マネジメントシステム及びＰＭＳ運用指針で要求されている文書化した情報に対し、以下の対策を行う

a)　必要な時に、必要な所で、入手可能かつ利用できるように、紙媒体は指定されたキャビネットに保管、また電子データは共用サーバの専用フォルダなどに保管する。

b)　紙媒体を保管したキャビネットは施錠管理を行う。
共用サーバの専用フォルダに保管している電子データは、アクセス権限やアクセ許可範囲で不要な変更への対策を行う。

(2) 文書化した情報の管理にあたっては、次の事項を実施する。
具体的な手順は、本規程 J.4.5.3 に定める。

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

(3) 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、健康推進機構内で作成した文書と同様に管理する。

### J.4.5.3 文書化した情報（記録を除く）の管理（JISQ150017.5.2、附属書 A.3.5.2）

(1) 健康推進機構は、ＰＭＳ運用指針が要求する全ての文書化した情報（記録を除く。）を管理する手順を、実施し、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

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

(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、健康推進機構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、改訂内容を健康推進機構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。

### J.4.5.4 内部規程（JISQ15001 附属書 A.3.3.5）

(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
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
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
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
e) 緊急事態への準備及び対応に関する規定
f) 個人情報の取得、利用及び提供に関する規定
g) 個人情報の適正管理に関する規定
h) 本人からの開示等の請求等への対応に関する規定
i) 教育などに関する規定
j) 文書化した情報の管理に関する規定
k) 苦情及び相談への対応に関する規定
l) 点検に関する規定
m) 是正処置に関する規定
n) マネジメントレビューに関する規定
o) 内部規程の違反に関する罰則の規定
p) 医療システム（電子カルテだけではなく、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）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健康推進機構のＰＭＳ規程全体で対応し、「医療情報システムの安全管理に関するガイドライン」、「保険医療福祉分野のプライバシーマーク認定指針第 4.1 版」を参照する
※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、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する。

### J.4.5.5 文書化した情報のうち、記録の管理（JISQ15001 附属書 A.3.5.3）

(1) 個人情報保護管理者は、健康推進機構の個人情報保護マネジメントシステム及びＰＭＳ運用指針の要求事項への適合を実証するために、以下に示す必要な記録を作成し、かつ、維持するものとする。

(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) 運用の確認の記録
  j) ＰＭＳ内部監査実施報告書
  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。
(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。
(5) 記録の廃棄について、保管期間が経過した記録は確実に消去・廃棄し、「ＰＭＳ記録管理台帳」に基づき対応する。

## J.5 運用

### J.5.1 運用（JISQ150018.1、8.2、8.3、附属書 A.3.4.1）

(1) 健康推進機構は、本指針の要求事項を満たすため及び J.3 で計画した活動について、実施するものとする。
(2) 健康推進機構は、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るものとする。
(3) 健康推進機構は、外部委託した業務がある場合は、管理の対象とする。
(4) 個人情報保護管理者は本項(1)～(3)についての記録を保持する。

## J.6 パフォーマンス評価（表題）

### J.6.1 監視、測定、分析及び評価（JISQ150019.１、附属書 A.3.7.1）

(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。

(2) 健康推進機構は、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、次の事項を決定する。

a) 対象とする個人情報保護マネジメントシステムの運用状況

b) “a)”で対象とした運用状況の監視、測定、分析及び評価の方法

c) “a)”で対象とした運用状況の監視及び測定の実施時期

d) “a)”で対象とした運用状況の監視及び測定の実施者

e) “a)”で対象とした運用状況の分析及び評価の時期

f) “a)”で対象とした運用状況の分析及び評価の実施者

(3) 健康推進機構は、次の事項について「運用確認記録」により、毎月１回確認し、その結果を個人情報保護管理者に報告し、承認を得るものとする。運用の確認は、各部門長及び情報システム管理者が行う。

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

(4) 確認した結果に不適合を確認した場合は、本規程 J.7.1 に基づき、是正処置を行う。

(5) 各部門は、監視及び測定の結果の証拠として、文書化した情報を定められた期間保管する。

(6) 個人情報保護管理者は、不適合が発見された場合には適時に、またそれ以外の場合は理事長によるＰＭＳの見直しに資するため、定期的に理事長にその状況を報告する。

### J.6.2 内部監査（JISQ150019.2、附属書 A.3.7.2）

(1) 健康推進機構は、個人情報保護マネジメントシステムが以下の事項の状況にあるか否かについて、少なくとも年一回、「ＰＭＳ内部監査計画書」に基づき内部監査を実施する。また、必要に応じて適宜に内部監査を実施する。標準的な実施時期は以下の通りとする。

a) 適合性監査：１１月

b) 運用状況の監査：１０月

(2) 個人情報保護監査責任者は、内部監査の実施に当たり、次の事項を行う。

c) 内部監査実施計画を策定、確立、実施及び維持する。その内部監査実施計画は、関連するプロセスの重要性及び前回までの監査の結果を考慮する

d) 計画時に、監査基準及び監査範囲を明確にする

e) 監査プロセスの客観性及び公平性を確保する監査員を選定し、内部監査実施計画に従って、内部監査を実施する

なお、監査員が、自己の所属する部署の内部監査を行わないよう、監査対象部門を割り当てる。

f) 内部監査の結果を監査報告書としてまとめ、管理層及びトップマネジメントに報告する

g)　内部監査実施計画及び監査結果の証拠として、文書化した情報を保持する

(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) 監査に関する詳細は以下の通りとする。

① 監査対象範囲

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。監査計画は J.3.3 により作成する。

②　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 J.3.1.3 個人情報保護リスクアセスメント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。

③ 監査の実施

監査員は、「ＰＭＳ内部監査計画書」に基づき、「ＰＭＳ内部監査チェックリスト（適合性及び運用監査)」を用い、現場責任者へのヒアリング、文書記録類の確認、現場視察により監査を実施する。

顧客内の就業場所の監査にあたり、顧客から監査員の立ち入りを拒否された場合、その就業場所の「運用確認記録」の結果を、内部監査の結果として用いるものとする。

④ 監査報告

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J.7.1是正処置の手順に従う。

⑥ 監査記録の保管
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。

### J.6.3 マネジメントレビュー（JISQ150019.3、附属書A.3.7.3）

(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) 前回までのマネジメントレビューの結果を踏まえた見直しの状況
b) 個人情報保護マネジメントシステムに関連する外部及び内部の問題点の変化
c) 以下の状況を踏まえた、現在の個人情報保護マネジメントシステムの運用状況の評価
1) 不適合及び是正処置
2) 確認及び点検の結果
3) 監査結果
4) 個人情報保護目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

(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 a)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)～f)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。

## J.7　改善

### J.7.1 不適合及び是正処置（JISQ1500110.1、附属書 A.3.8）

(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) その不適合に対処し、該当する場合には、必ず、次の事項を行う。

1)その不適合を管理し、修正するための処置をとる。

2)その不適合によって起こった結果に対処する。

b) 次の事項によって、その不適合の原因を除去するための処置を検討する。

1)その不適合を調査及び分析する。

2)その不適合の原因を特定する。

3)類似の不適合の有無、又はそれが発生する可能性を検討する。

c) 是正処置を計画し、計画された処置を実施する。

d) 実施された全ての是正処置の有効性を調査、分析及び評価する。

e) 必要な場合には、個人情報保護マネジメントシステムの改善を行う。

(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。

### J.7.2 継続的改善

(1) 健康推進機構は、マネジメントレビューの結果などに基づき、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くものとする。

## 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（JISQ15001 附属書 A.3.4.2.1）

(1) 個人情報を取り扱うに当たっては、そ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行う。

(2) 利用目的等の特定に当たっては、取得した情報及びデータの紐づけにより確認され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、本人に通知するか容易に参照できるように公表するなどの対策を行う。

(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。

(4) 健康推進機構は、個人情報の公序良俗に反する利用は行わない。

(5) 利用目的等の特定手順

①既存の個人情報は、個人情報の特定時に「個人情報管理台帳」に利用目的を明記し、

個人情報保護管理者の承認を得る。

② 新種の個人情報は、「個人情報取扱申請書」に利用目的を明記し、個人情報保護管理者の承認を得た後、「個人情報管理台帳」に記録する。

③ なお、取得する個人情報が、項目ごとにその利用目的が異なる場合、利用目的は項目ごとに区別して特定する

④ 利用目的を変更する際の手順は、J.8.6(5)に定める。

### J.8.2 適正な取得（JISQ15001 附属書 A.3.4.2.2）

(1) 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。

(2) 個人情報を本人から取得する場合には、J.8.4(2)の a)～d)の場合を除いて、利用目的を本人への利用目的の通知または公表などを行う。

(3) 個人情報を本人以外から取得する場合で、委託・提供・共同利用により個人情報を取得する場合は、委託元・提供元またはその他の共同利用者が個人情報保護法及び個人情報保護委員会のガイドライン等に沿って適切に個人情報を取り扱っていることを事前に確認し、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。

(4) 個人情報を取得する場合には、事前に次に示す取得に該当しないか確認するものとする。

a) 利用目的を偽るなど不公正な手段によって個人情報を取得すること。

b) 優越的な地位を利用して個人情報を取得すること。

c) 十分な判断能力のない状態の者(子供、身障者、高齢者、心身膠着状態の者等)から取得すること。

d) 委託元の許可を得ていないマイナンバーの再委託を受けること。

(5) 本人等以外の情報を本人等から得る場合は、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、本人等以外から本人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等と取得状況の説明を行う。

(6) 意識障害、精神障害、乳幼児などで、説明により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。

(7) 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。

### J.8.3 要配慮個人情報（JISQ15001 附属書 A.3.4.2.3）

(1) 健康推進機構は、新たに要配慮個人情報を取得、利用又は提供並びに要配慮個人情報のデータを提供する場合、あらかじめ書面による本人の同意を得るものとする。ただし、本項(2)、(3)に該当する場合を除く。

(2) 要配慮個人情報を取得、利用する際、書面による本人の同意を得ることを要しないとき

とは、以下の場合に限定する。

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) 当該要配慮個人情報が、法令等により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であるとき

f) 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得又は利用する場合

g) 個人情報保護法 27 条第 5 項各号に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき

h) 個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

i) 学術研究機関等から当該要配慮個人情報を取得し、利用する場合であって、当該要配慮個人情報を学術研究目的で取得し、利用する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）

(3) 要配慮個人情報を提供する際、書面による本人の同意を得ることを要しないときとは、本項(2)の a)～d)、または以下の場合に限定する。

j) 個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

k) 個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）

l) 第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的であ

る場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

(4) 取得、利用の場合は本項(2)の a)～i)を、提供の場合は本項(2)の a)～ｄ)又は本項(3)の j)～l) を本人の同意が不要な場合とし、適用する場合には、「個人情報例外適用申請書」に適用するただし書きを記載し、個人情報保護管理者の承認を得る。

### J.8.4 個人情報を取得した場合の措置（JISQ15001 附属書 A.3.4.2.4）

(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し、又は公表するものとする。ただし、本項(2)に該当する場合は、この限りではない。

(2) 本人に利用目的を通知し、又は公表を要しないのは、以下の場合に限定する。

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健康推進機構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

(3) 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。

### 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（JISQ15001 附属書 A.3.4.2.5）

(1) 健康推進機構は、J.8.4 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、書面によって本人

の同意を得るものとする。ただし、本項(2)に該当する場合を除く。

a) 事業者の名称又は氏名

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) J10.4～J10.7 に該当する場合には、その請求等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) 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、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、又は J.8.4 (2) の a)～d)のいずれかの場合に限定する。

(3) 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。

6)電話による個人情報の直接取得等においても、上記内容を通知し同意を得る。但し本人への医療の提供のために保健医療福祉サービスの遂行上必要な範囲の利用目的の同意は健康推進機構内掲示で明示し、原則として黙示による同意を得ることとする。

### J.8.6 利用に関する措置（JISQ15001 附属書 A.3.4.2.6）

(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) 健康推進機構は、(1)に該当する場合でも、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、または誘発するおそれがある方法により個人情報を利用しない。

(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、J.8.5(1)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、本人の同意を得る。ただし、本項(4)に該当する場合を除く。

(4) 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、次の場合に限定する。

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り当該事務の遂行に支障を及ぼすおそれがあるとき。

e) 当該個人情報取扱事業者が学術研究機関等である場合であって、学術研究目的で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

f) 学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

(5) 社内承認の手続き

① 利用目的を変更する場合、「個人情報取扱い同意書面」に必要事項を記入の上、利用目的を改訂したJ.8.5(1)a)～f)の通知事項を含む同意書様式を作成・添付し、部門管理責任者を経由して、個人情報保護管理者の承認を得る。

② 本項(4)の項目を適用し、本人の同意を得ない場合は、「個人情報例外適用申請書」に適用するただし書きを記載し、部門管理責任者を経由して、個人情報保護管理者の承認を得る。

(6) 目的外利用に該当するかどうか疑わしい場合には、個人情報保護管理者に相談し、指示を仰ぐものとする。

### J.8.7 本人に連絡又は接触する場合の措置（JISQ15001 附属書 A.3.4.2.7）

(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、J.8.5(1)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。ただし、本項(2)に該当する場合を除く。

(2) 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を、利用する個人情報が以下の場合に限定する

a) J.8.5(1)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組織が、既にJ.8.5(1)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、共同して利用する者が、既にJ.8.5(1)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、本人に通知するか、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及び住所並びに法人にあっては、その代表者の氏名
- 取得方法

e) J.8.4(1)の 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) J.8.3(2)の a)～d)のいずれかに該当する場合

(3) 社内承認の手続き

① 本人に連絡又は接触する場合は「個人情報取扱申請書」に必要事項を記入し、利用目的の変更内容及び取得方法を明記した同意書様式を作成・添付し、当該個人情報を用いて本人に連絡又は接触することを個人情報保護管理者の承認を得る。

② 本人に連絡又は接触する目的が、J.8.6(3)に該当する場合は、J.8.6 に基づき、利用目的変更の手続きを行う。

③ (2)の b)～f)に該当するため本人への通知と同意を要しない場合は、「個人情報取扱申請書」に適用するただし書きを記載し、個人情報保護管理者の承認を得る。

(4) 本人からの同意取得方法

本人に文書等により、当該個人情報を用いて連絡又は接触する必要が生じたことを説明し、作成した同意書様式を送付し同意文書を返送により取得する。

なお、書面で同意を得ることができない場合は、口頭で同意を得ても良いが、同意を得た記録を書面にて残すこととする。

(5) 本項(2)の d)を適用する場合

健康推進機構は個人情報の共同利用を行わない。

もし、共同利用する必要が生じた場合には、共同利用に関する必要事項を記載してウェブページに掲載し、本人が容易に知りうる状態におく。

### J.8.8 個人データの提供に関する措置（JISQ15001 附属書 A.3.4.2.8）

(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、J.8.5(1)a)～d)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、本項(2)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。

(2) 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、以下の場合に限定する。

なお、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ときは、法令等の定めに基づき、法令等で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

a) J.8.5の規定によって、既にJ.8.5(1)a)～d)の事項又はそれと同等以上の内容の事項を本人に明示又は通知し、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) 健康推進機構の名称及び住所並びにその代表者の氏名
2) 第三者への提供を利用目的とすること
3) 第三者に提供される個人データの項目
4) 第三者への提供の手段又は方法
5) 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
6) 第三者に提供される個人データの取得の方法
7) 本人からの請求などを受け付ける方法
8) その他個人の権利利益を保護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事項

ただし、以下に対して本項は適用しない

①要配慮個人情報

②偽りその他不正の手段により取得された個人データ

③個人情報保護法27条第2項、又は本項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。）

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、本人又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)～8)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置いているとき

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、J.8.7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)　J.8.3(2)の a)～d)のいずれかに該当する場合

(3) 社内承認の手続き

①　個人データを第三者へ提供する場合は、「個人情報取扱申請書」に必要事項を記入し、取得方法及び第三者提供の要領を明記した同意書様式を作成・添付し、当該個人情報を用いて第三者に個人データを提供することを個人情報保護管理者の承認を得る。

②　個人データを第三者へ提供する目的が、J.8.6(3)に該当する場合は、J.8.6 に基づき、利用目的変更の手続きを行う。

③　(2)の b)～g)に該当するため通知と同意を要しない場合は「個人情報例外適用申請書」に適用するただし書きを記載し、個人情報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) 本人からの同意取得方法

本人に文書等により、当該個人情報を提供する必要が生じたことを説明し、作成した同意書様式を送付し同意文書を返送により取得する。

なお、書面で同意を得ることができない場合は、口頭で同意を得ても良いが、同意を得た記録を書面にて残すこととする。

(5) 原則的に、本項(2)の項目 b)（オプトアウトによる個人データの提供）は適用しない。

適用する場合は、第三者に提供する個人データ（要配慮個人情報を除く）を、本人の求め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としている場合であって、次に掲げる事項について個人情報保護委員会規則で定めるところにより、予め本人に通知し、又は健康推進機構ウェブページに掲載し、本人が容易に知り得る状態に置くと共に、個人情報保護委員会に届け出たときは、前項の規定にもかかわらず、当該個人データを第三者に提供することができるものとする。

1)　健康推進機構の名称及び従所並びにその代表者の氏名

2)　第三者への提供を利用目的とすること

3)　第三者に提供される個人データの項目

4)　第三者に提供される個人データの取得の方法

5)　第三者への提供の手段又は方法

6)　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

7)　本人からの請求などを受け付ける方法

8)　その他法令等で定める事項

(6) 健康推進機構は本項(2)の項目 c)を適用することはない。

もし、c)を適用する必要が生じた場合には、第三者提供に関する必要事項を記載して健

康推進機構ウェブページに掲載し、本人が容易に知りうる状態におく。

(7) 本項(2)の項目 f)を適用する場合

健康推進機構は個人情報の共同利用を行わない。もし、共同利用する必要が生じた場合には、共同利用に関する必要事項を記載して健康推進機構ウェブページに掲載し、本人が容易に知りうる状態におく。

また、共同利用会社間で J.8.7d) に規定されている共同利用に関する事項について契約を締結すること。

### J.8.8.1 外国にある第三者への提供の制限（JISQ15001 附属書 A.3.4.2.8.1）

(1) 外国にある第三者に個人データを提供する場合、以下のいずれかを満たしていることを確認したうえで行う。ただし、J.8.3(3)の a)～d)、又は、J.8.3(4)の j)～l)のいずれかに該当する場合を除く。

a) 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がある場合

b) 個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ず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適合する体制を整備している者への提供をする場合

c) 個人の権利利益を保護する上で我が国と同等の水準にある外国として個人情報保護委員会規則で定める国・地域にある第三者への提供をする場合

(2) 本項(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、法令等の定めるところによって、次に掲げる事項について、当該本人に必要な情報を提供したうえで同意を得る。

d) 当該外国の名称

e) 当該外国における個人情報の保護に関する制度に関する情報

f) 当該第三者が講ずる個人情報の保護のための措置に関する情報

g) d)～f)に定める事項が特定できない場合、その旨及びその理由

h) g)に該当する場合について、d)～f)の事項に代わる本人に参考となるべき情報がある場合には、当該情報

i) g)及び h)に該当する場合であって、情報提供できない場合には、g)及び h)に定める事項に代えて、その旨及びその理由

(3) 本項(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には、あらかじめ、法令等の定めるところによって、次に掲げる事項について、必要な措置を講じる。

j) 当該第三者による相当措置の実施状況並びに相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容について、適切かつ合理的な方法による定期的な確認

k) 当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人デ

ータの当該第三者への提供の停止

1) 本人の求めを受けた場合には、情報提供することにより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を除き、遅滞なく、以下の情報の提供

1) 当該第三者による体制の整備の方法

2) 当該第三者が実施する相当措置の概要

3) j)による確認の頻度及び方法

4) 当該外国の名称

5) 当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要

6) 当該第三者による相当措置の実施に関する支障の有無及びその概要

7) 前号の支障に関して、k)により講ずる措置の概要

(4) 本項(3)の 1)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、その理由を説明する。

(5) 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。

### J.8.8.2 第三者提供に係る記録の作成など（JISQ15001 附属書 A.3.4.2.8.2）

(1) 健康推進機構は、個人データを第三者に提供したときに、法令等の定めるところによって「個人データ第三者提供記録」を作成する。ただし、次に掲げるいずれかに該当する場合は、記録の作成を要しない。

a) 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

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

c) 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、J.8.7 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

d) 法令に基づく場合

e) 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

f) 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

g) 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

h) 個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

i) 個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利を不当に侵害するおそれがある場合を除く。）（個人贋報取扱事業者と第二者が共同して学術研究を行う場合に限る。）

j) 第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

(2) 本項(2)の a)～j)いずれかに該当する場合は、「個人情報例外適用申請書」に第三者提供の目的、相手企業名、適用するただし書きを記載し、個人情報保護管理者の承認を得る。

(3) 第三者提供の記録の保持

「個人データ第三者提供記録」を作成した場合、個人情報保護管理者の承認を受け、当該記録を必要な期間保管する。

記録に残す内容は以下のとおりとする。

| | 提供年月日 | 第三者の氏名等 | 本人の氏名等 | 個人データの項目 | 本人の同意 |
|---|---|---|---|---|---|
| オプトアウトによる第三者提供 | ○ | ○ | ○ | ○ | |
| 本人の同意による第三者提供 | | ○ | ○ | ○ | ○ |

なお、「個人情報の保護に関する法律施行規則」第 19 条第 2 項に基づき、継続的に若しくは反復して提供する場合は、一括して作成することも出来る。また、同第 3 項に該当する場合は、当該提供に関して作成された契約書その他の書面をもって記録に代えることができるものとする。また、記録方法、記録媒体、記録事項、保存期間などは同規則の第 15 条～18 条によるものとする。

(4) 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、適切に応じるものとする。

### J.8.8.3 第三者提供を受ける際の確認など（JISQ15001 附属書 A.3.4.2.8.3）

(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、法令等の定めるところによって、必要な確認を行う。ただし、本項(2)に該当する場合を除く。

(2) 第三者から個人データの提供を受けるに際して、確認を要しないのは、以下の場合に限定する

a) 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されたとき

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を提供される場合であって、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

c) 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、J.8.7 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

d) 法令に基づく場合

e) 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

f) 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

g) 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

h) 個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

i) 個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利を不当に侵害するおそれがある場合を除く。）（個人贋報取扱事業者と第二者が共同して学術研究を行う場合に限る。）

j) 第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

(3) 社内承認の手続き

① 本項(2)の a)～j)のいずれかに該当する場合は、「個人情報例外適用申請書」に第三者提供を受ける目的、相手企業名、記録を要しない理由に適用するただし書きを記載し、個人情報保護管理者の承認を得る。

(4) 第三者提供受領の記録の保持

第三者提供受領の都度、受領内容を確認し、「個人データ第三者提供受領記録」を作成し、

個人情報保護管理者の承認を受け保管するものとする。
記録に残す内容は以下のとおりとする。

| | 提供を受けた年月日 | 第三者の氏名等 | 取得の経緯 | 本人の氏名等 | 個人データの項目 | 個人情報保護委員会による公表 | 本人の同意等 |
|---|---|---|---|---|---|---|---|
| オプトアウトによる第三者提供 | ○ | ○ | ○ | ○ | ○ | ○ | |
| 本人の同意による第三者提供 | | ○ | ○ | ○ | ○ | | ○ |
| 私人などからの第三者提供 | | ○ | ○ | ○ | ○ | | |

なお、「**個人情報の保護に関する法律施行規則**」第 23 条第 2 項に、継続的に若しくは反復して提供を受けた時は、一括して作成することも出来る。また、同第 3 項に該当する場合は、当該提供に関して作成された契約書その他の書面をもって記録に代えることができる。また、確認方法、記録媒体、記録事項、保存期間などは同規則の第 15 条～18 条によるものとする。

### J.8.8.4 個人関連情報の第三者提供の制限など

(1) 健康推進機構は、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以下の様に定める。

(2) 提供先の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.8.3(3)の a)～d)、又は、J.8.3(3)の j)～l)のいずれかに該当する場合を除き、あらかじめ、次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、確認を行う。

a) 当該第三者が個人関連情報取扱事業者から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること。

b) 外国にある第三者への提供にあっては、a)の本人の同意を得ようとする場合において、法令等で定めるところによって、以下の 1)～3)に示す事項について、あらかじめ、当該本人に提供されていること。

1) 当該外国における個人情報の保護に関する制度
2) 当該第三者が講ずる個人情報の保護のための措置
3) その他当該本人に参考となるべき情報

(3) 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、契約を締結することなどで、講じる。

(4) 個人関連情報を提供する場合には、以下の事項について、確認の記録を作成、保管する。

① 個人関連情報の提供元の確認の記録事項

c) a)で本人の同意を得ている旨及び外国にある個人情報取扱事業者にあっては、本項(2)b)で本人に情報の提供が行われていることを確認した旨

d) 個人関連情報を提供した年月日

e) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

f) 当該個人関連情報の項目

② 個人関連情報の提供先の確認の記録事項

g) a)で本人の同意が得られている旨及び外国にある個人情報取扱事業者にあっては、b)で本人に情報の提供が行われている旨

h) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

i) 当該個人データ（個人関連情報）によって識別される本人の氏名その他当該本人を特定するに足りる事項

j) 当該個人関連情報の項目

### J.8.9 匿名加工情報

(1) 健康推進機構は、匿名加工情報の取扱いを行うか否かの方針を、以下のように定める。

a) 健康推進機構では当面の間、匿名加工情報の取扱いを行わない。

(2) 健康推進機構は、匿名加工情報を取り扱う場合には、本人の権利利益に配慮し、かつ、法令等の定めるところによって、以下に示す適切な取扱いを行う手順を確立する。

① 健康推進機構で匿名加工情報の取扱いを開始する際は、②～⑤遵守事項等の対処方法を社内で定められた稟議書等に記載して、個人情報保護管理者経由で理事長の承認を得るものとする。

② 匿名加工を行う場合は下記の事項を遵守する。

1) 匿名加工情報を作成する場合は下記③の適正な加工を行わなければならない。

2) 匿名加工情報を作成したときは加工方法等の情報の安全管理措置を講じなければならない。

3) 匿名加工情報を作成したときは、当該情報に含まれる情報の項目を公表しなければならない。

4) 匿名加工情報を第三者提供するときは、提供する情報の項目及び提供方法について公表すると共に、提供先に当該情報が匿名加工情報である旨を明示しなければならない。

5) 匿名加工情報を自ら利用するときは、元の個人情報に係る本人を識別する目的で他の情報と照合することを行ってはならない。

6) 匿名加工情報を作成したときは、匿名加工情報の適正な取扱いを確保するため、安全管理措置、苦情の処理などの措置を自主的に講じて、その内容を公表する

ように努めなければならない。

③ 匿名加工情報を作成する場合は下記の手順を実施する。

1) 特定の個人を識別することの出来る記述（例：氏名）等の全部又は一部を削除すること。
2) 個人識別符号（マイナンバー、運転免許証番号等）の全部を削除すること。
3) 個人情報と他の情報との連結する符号（例：委託先に渡すために分割したデータとひも付ける ID）を削除すること。
4) 特異な記述(例：年齢 116 歳や極少病歴など)を削除すること。
5) 以上のほか、個人情報とデータベースの内の他の個人情報との差異等の性質を勘案し適切な措置を講ずること。

④ 匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者が遵守すべき義務等は以下の通りする。

1) 匿名加工情報を第三者提供する時は提供する情報の項目及び提供方法について公表すると共に、提供先に当該情報が匿名加工情報である旨を明示しなければならない。
2) 匿名加工情報を利用するときは、元の個人情報に係る本人を識別する目的で、加工方法等の情報を取得し、又は他の情報と照合することを行ってはならない。
3) 匿名加工情報の適正な取扱いを確保するため、安全管理措置、苦情の処理などの措置を自主的に講じて、その内容を公表するように努めなければならない。

⑤ 匿名加工情報を取り扱っている場合には、その以下の確認の記録を作成、保管する

1) 匿名加工情報の取り扱いを定めた稟議書など
2) 匿名加工情報のもとになる個人情報及び加工方法
3) 匿名加工情報に含まれる情報の項目
4) 匿名加工情報を提供先及び提供方法、時期などの提供に関する項目
5) 苦情があった場合、その内容と対応内容

### J.8.10 仮名加工情報

(1) 健康推進機構では当面の間、仮名加工情報の取扱いを行わない。

(2) 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以下のように定める。

① 健康推進機構が仮名加工情報の取扱いを行う場合には、以下の②～⑦の遵守事項等の対処方法を社内で定められた稟議書等に記載して、個人情報保護管理者経由で理事長の承認を得るものとする。

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、個人情報を加工する。

1) 個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除する。（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
2) 個人情報に含まれる個人識別符号の全部を削除する。（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
3) 個人情報に含まれる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記述等を削除する。（当該記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

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る。
1) 個人情報保護管理者が任命した担当者が、削除情報等を取り扱う。
2) 削除情報等の取扱いは、本規程及び「**安全管理規程**」に基づいて取り扱うものとする。
3) 削除情報等の取扱う担当者は、J.6.1に基づき、削除情報などの取扱い状況を確認し、個人情報保護管理者に報告するものとする。
4) 削除情報等の取扱う担当者及び個人情報保護管理者は、J.6.1に基づき確認した際に、不備、不適合を発見した場合は、J.7.1に基づき是正処置を行う。

④ 仮名加工情報を利用する場合には、以下を実施すること。仮名加工情報を利用する場合には、以下を実施する。
a) 利用目的をできる限り特定し、法令に基づく場合を除くほか、その目的の達成に必要な範囲内において行う。
b) あらかじめその利用目的を公表している場合及び法令に基づく場合を除き、速やかに、その利用目的を公表する。
c) 仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合しない。
d) 電話をかけ、郵便若しくは信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用しない。

⑤ 仮名加工情報を提供する場合には、以下の場合を除き、仮名加工情報である個人データを第三者に提供を行わない。
e) 仮名加工情報の取扱いの全部又は一部を、J.9.4と同等の措置を講じたうえで委託する場合

f) 仮名加工情報が特定の者との間で共同して利用され、共同して利用する者が、既に共同して利用する場合（J.8.5(1)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、以下の1)～6)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く場合）

1) 共同して利用すること
2) 共同して利用される仮名加工情報の項目
3) 共同して利用する者の範囲
4) 共同して利用する者の利用目的
5) 共同して利用する仮名加工情報の管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
6) 取得方法

g) 合併その他の事由による事業の継承に伴って仮名加工情報を提供する場合

(3) 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う。
苦情の対応に関してはJ.11.1に準ずる。

(4) 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する。

## J.9 適正管理

### J.9.1 正確性の確保（JISQ15001 附属書 A.3.4.3.1）

(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ものとする。

(2) 健康推進機構は、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を含む管理を、規定に基づいて適切に行うものとする。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。

### J.9.2 安全管理措置（JISQ15001 附属書 A.3.4.3.2）

(1) 健康推進機構は、個人情報保護管理者を通じて、その取り扱う個人情報のリスクに応じ

て、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために法令に基づき、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。

### J.9.3 従業者の監督（JISQ15001 附属書 A.3.4.3.3）

(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。

(2) 従業者とのとの雇用契約時に、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。

(3) 「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。

(4) ＰＭＳに違反した場合は、「就業規則」の懲戒条項を適用する。

(5) 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、総務課長とする

－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。

### J.9.4委託先の監督（JISQ15001 附属書 A.3.4.3.4）

(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。

## 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（JISQ15001 附属書 A.3.4.4.1）

(1) 健康推進機構は、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付けた場合、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) J.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ること。

(3) 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。

(4) (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。

**J.10.2 開示等の請求等に応じる手続（JISQ15001 附属書 A.3.4.4.2）**

(1) 健康推進機構は、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として以下の事項を定める。

a) 開示等の請求等の申し出先

b) 開示等の請求に際して提出すべき書面の様式とその他の開示等の請求の方式

c) 開示等の請求をする者が、本人又は代理人であることの確認の方法

d) J.10.4 又は J.10.5 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、本人の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、J.10.4 又は J.10.5 によって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、その額を定めるものとする。

(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 開示等の請求の申し出先

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 本人又は代理人であることの確認方法

a) 個人情報の開示等の請求に応じる場合の本人確認

以下の本人確認書類のいずれかの写しを同封することとする（本籍地の情報は都道府県のみとして、その他は黒塗りで収集するものとする）。

・運転免許証

・マイナンバーカード（表面）

・その他本人確認できる写真入りの公的証明書

b) 代理人による開示等の請求の場合

代理人による開示等の請求の場合、代理権が確認できる下記 1)の書類の写しいずれか及び代理人自身を証明する 2)の書類の写しのいずれかを必要とする。

1) 代理人である事を証明する書類

＜開示等の請求をすることにつき本人が委任した代理人の場合＞

- 本人の委任状

＜代理人が未成年者の法定代理人の場合＞

- 戸籍謄本
- 登記事項証明書
- その他法定代理権の確認ができる公的書類

＜代理人が成年被後見人の法定代理人の場合＞

- 後見登記等に関する登記事項証明書
- その他法定代理権の確認ができる公的書類

2) 代理人自身を証明する書類（本籍地の情報は都道府県のみとして、その他は黒塗りで収集するものとする。）

- 運転免許証
- マイナンバーカード（表面）
- その他本人確認できる写真入りの公的証明書

④ 開示等の請求の手数料および徴収方法

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。

### J.10.3 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

（JISQ15001 附属書 A.3.4.4.3）

(1) 健康推進機構は、保有個人データに関し、次の事項を本人が知り得る状態（本人の求めなどに応じて遅滞なく回答する場合を含む）に置く

a) 健康推進機構の名称及び住所並びに法人にあっては、その代表者の氏名

b) 個人情報保護管理者（若しくは代理人）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（J.8.4(1)の a)～c)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し出先

e) 健康推進機構の属する認定個人情報保護団体の対象事業社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) J.10.2 によって定めた手続き

g) 保有個人データの安全管理のために講じた措置（本人の知り得る状態に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）

(2) 本人が知り得る状態とする方法

① (1)の a)～g)の事項については、健康推進機構ウェブページにて公表することとする。

② 本人からの求めがあった場合には苦情・相談窓口責任者が応じることとし、遅滞なく文書にて送付することとする。

### J.10.4 保有個人データの利用目的の通知（JISQ15001 附属書 A.3.4.4.4）

(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、J.8.4 のただし書き a)～c)のいずれかに該当する場合、又は 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。

(2) 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。

(3) 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。

(4) 本項(2)に該当する場合は、利用目的通知の求めに応じない場合、その理由の説明について立案し、「個人情報開示等請求回答書」に記入する。

① 「個人情報開示等請求回答書」の記入内容について、個人情報保護管理者の承認を得る。

② 利用目的についての本人への回答（求めに応じない場合はその旨の回答と③で立案した理由の説明）は以下のいずれかの適切な方法を選択し行う。

a) 登録されている本人住所に回答文面を郵送する。

b) 登録されている本人の FAX 番号に回答文面を FAX する。

c) 登録されている本人のＥメールアドレスに回答文面をメールする。

d) 登録されている本人の電話番号に電話をかけ、口頭にて回答する。

### J.10.5 保有個人データ又は第三者提供記録の開示（JISQ15001 附属書 A.3.4.4.5）

(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）によって開示するものする。ただし、本項(2)に該当する場合を除く。

(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

なお、上記内容で請求に応じない場合は、本人に遅滞なくその旨を通知するとともに、理由の説明を行う。

(3) 本項(1)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、本項(2)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、理由を説明する。

(4) 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。

### J.10.6 保有個人データの訂正、追加又は削除（JISQ15001 附属書 A.3.4.4.6）

(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。

(2) 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。

(3) 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。

### J.10.7 保有個人データの利用又は提供の拒否（JISQ15001 附属書 A.3.4.4.7）

(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、J.10.5 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。

(2) 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。

(3) 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。

## J.11　苦情及び相談への対応

### J.11.1 苦情及び相談への対応（JISQ15001 附属書 A.3.6）

(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。なお、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、当該団体の苦情解決の申し出先も明示すること。

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Ｐ ＭＳ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。

## J.12　雑則

### J.12.1 改廃

本規程の改廃は、個人情報保護管理者によって起案され、理事長によって承認されるもの

とする。

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。

４　この規程は、令和６年４月１日から施行する。

５　この規程は、令和７年４月１日から施行する。