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

一般財団法人 医療情報システム開発センター
Medical Information System Development Center

改定履歴

版数	日付	内容
第 1 版	平成 18 年 10 月 19 日	JIS Q 15001:2006 に準拠した認定指針として発行
第 2 版	平成 20 年 10 月 1 日	本文：審査の実績から、審査で確認する内容は、できるかぎり”C．最低限のガイドライン”に反映した。また、”3.4.3.2 安全管理措置”、”3.7.2 監査”、”3.8 是正措置及び予防措置”の内容を重点的に見直した。 付録：第１版の付録９～１３（申請の様式等）を削除し、「医療情報システムの安全管理に関するガイドライン・第３版」の要約を別冊として巻末に添付した。
第 2.1 版	平成 22 年 4 月 1 日	一部表現の修正、及び「医療情報システムの安全管理に関するガイドライン」第３版の要約を、4.1 版の第６章等と差し替える。
第 3 版	平成 23 年 1 月 26 日	匿名化や共同利用等の考え方の明確化、および表現の追加・修正。同意書、個人情報取扱申請書、個人情報管理台帳、及びリスク分析表等の個人情報の特定、リスク分析に係る様式例を追加・修正。
第 3.1 版	平成 23 年 7 月 1 日	一部表現の修正。JIS Q 15001:2006 の解説修正に整合を取る。「是正処置及び予防処置」、「代表者による見直し」の様式例の追加。
第 3.2 版	平成 25 年 3 月 25 日	付録１０削除。一部表現の修正。付録３ 、付録５～１３ 、付録１５、付録１７～２０、付録２５の追加・変更。
第 3.3 版	平成 27 年 2 月 1 日	平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号に対応。付録 26 を「医療情報システムの安全管理に関するガイドライン」第 4.2 版の抜粋に差し替える等。
第 4 版	平成 30 年 4 月 1 日	全般：JIS Q 15001:2017 に準拠した内容に変更。その他、審査の実績、法令・ガイドラインへの対応によりＢ．Ｃ．Ｄ．及び付録の内容を見直した

目　次

※ＨＰ公表版には付録１～２６及び用語解説は掲載しておりません

はじめに

プライバシーマーク制度とは

個人情報をコンピュータに蓄積し、ネットワークを通じて交換するネットワーク社会では、さまざまな媒体やネットワークサービスなどを通じて多くの個人情報が拡散することや、不正に入手した個人情報が悪用されることなど、従来にないプライバシーの侵害が行われることが懸念される。わが国では、1988 年に公的機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」（以下、「88 年法」という）が公布されたことにより、初めてプライバシー保護に係る法律が制定された。しかし、民間部門は対象ではないことから、1989 年に民間部門に対して通産省（現:経済産業省）により「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（以下、「民間部門 GL」という）が策定された。しかし 88 年法には罰則規定が無く、また民間部門 GL には法的拘束力が無く自主的な規制に頼るなど、これらは個人情報保護制度という観点から満足できるものではなかった。

その後、自主規制の更なる推進の必要から、あらゆる産業分野に適用する国内基準として、1999 年 3 月に民間部門 GL をベースとした日本工業規格「JIS Q 15001:1999 個人情報に関するコンプライアンス・プログラムの要求事項」が制定された。JIS Q 15001 には利用方法として、事業者が自己の個人情報保護の取組みが JIS Q 15001 に適合していることを自ら評価するために用いることができるとともに、第三者による評価の基準としても活用できることとされている。このことから、（財）日本情報処理開発協会（現：「一般財団法人日本情報経済社会推進協会」以下、「JIPDEC」という）は、既に民間部門 GL を基準として 1998 年 4 月からスタートしていた「プライバシーマーク制度」を、新たに JIS Q 15001 を基準とした第三者認証制度とした上で、プライバシーマーク制度の本格運用を開始した。

プライバシーマーク制度は、個人情報を取り扱う事業者等の個人情報の適切な取り扱いを促進することを目的とした制度で、JIS Q 15001 に基づく個人情報の適切な保護措置を講ずる体制を整備している事業者等に対し、その申請に基づいて審査を行い、認定の旨を示すプライバシーマークを付与することにより、事業活動に際してプライバシーマークの使用を認める制度である。

認定指針作成の経緯

JIS Q 15001 は、あらゆる産業分野に適用することが可能であるが、そのために特定の産業分野に偏らない内容となっている。一方、分野によっては個人情報の取扱いにおいて、その分野独自の慣行等特殊な事情があることから、JIS Q 15001 の適用においてはその分野の特殊性を勘案しなければならない。特に、個人情報の取扱いが複雑で多岐にわたっている医療関連機関においては、この傾向が強い。そのため、医療分野の個人情報保護の推進を加速させることを目的として、JIPDEC は、医療分野の専門家による「医療機関の

認定指針検討 WG」を設定して、医療分野に JIS Q 15001 を適用する際のガイドラインとなる解説書を作成し、2002 年 10 月に「医療機関の認定指針」として公表した。

2003 年 7 月に（一財）医療情報システム開発センター（以下、「MEDIS-DC」という）がプライバシーマーク付与認定審査指定機関に指定され、「医療機関の認定指針」に基づく保健医療福祉分野の事業者に対する付与認定審査を実施している。その後、2004 年 12 月に厚生労働省が「医療・介護関係事業者における個人情報保護の適切な取扱いのためのガイドライン」（以下、「厚生労働省のガイドライン」という）を公表、2005 年 4 月の「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下、「個人情報保護法」という）の全面施行等、個人情報保護に関する大きな情勢変化があった。さらに 2006 年 5 月 20 日には JIS Q 15001 が改訂され、「JIS Q 15001:2006 個人情報保護マネジメントシステム－要求事項」として公表された。

これらのことをふまえ「医療機関の認定指針」を改訂することとした。改訂に当たっては、これまでの保健医療福祉分野の付与認定審査の実績から、（一財）医療情報システム開発センターが当たることとし、保健医療福祉分野の専門家による「医療機関の認定指針・改訂委員会」*を設置して検討し、従来の「医療機関の認定指針」を見直し、「保健医療福祉分野のプライバシーマーク認定指針」（以下、「認定指針」という）とした。

JIS Q 15001 の改訂と認定指針第 4 版への改訂

「個人情報保護法」の全面施行以来、10 年以上にわたり実質的な改正は行われてこなかったが、その間、情報通信技術の発展に伴い個人情報の利用形態も多種多様になり膨大なパーソナルデータの収集・分析が行われるなど、個人情報保護法制定時には想定されていなかった個人情報の利用が行われるようになってきた。

しかしながら、個人情報が広く利活用される一方で、個人情報に該当するかどうかの判断が困難ないわゆるグレーゾーンの為に、事業者による個人情報の利活用が躊躇される状況が見られることや、消費者によるプライバシーの権利意識が高まってきているのと比例して、事業者における個人情報の取扱いについての懸念も増大しているなどの問題点も顕在化してきた。

これらの状況に鑑み、個人情報の保護にも配慮しつつ、パーソナルデータの利活用のためのデータ利用環境の整備と、国民の安全・安心の向上の実現のために、個人情報保護法が平成 27 年 9 月に改正され平成 29 年 5 月 30 日施行された。

また、改正個人情報保護法の施行に先立ち、平成 27 年 10 月 5 日に「行政手続き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の一部を改正する法律」（マイナンバー法）が施行され、平成 28 年 5 月には、カルテや診療報酬明細等の医療情報に番号制度を導入する方針が正式に決定された。

さらには、個人情報保護法の改正を踏まえ、平成 29 年 12 月 20 日には「JIS Q 15001:2017 個人情報保護マネジメントシステム－要求事項」が公表された。

これらのことをふまえ、「認定指針」も改正個人情報保護法と新 JIS の内容を反映させた形で大幅に内容を見直し第４版を発行することとした。

*「保健医療福祉分野のプライバシーマーク認定指針・改訂委員会」の構成

（当時の所属・肩書き）

＜主査＞

国立研究開発法人　国立国際医療研究センター
医療情報管理部門　部門長　美代　賢吾

＜委員＞（５０音順）

株式会社 富士通マーケティング・エージェント
主席コンサルタント　蒲池　直樹

一般財団法人 日本情報経済社会推進協会
プライバシーマーク推進センター　制度企画グループ
上河辺　康子

一般社団法人 保健医療福祉情報安全管理適合性評価協会
理事長　喜多　紘一

社会保険診療報酬支払基金
本部　理事　清谷　哲朗

プライバシーマーク主任審査員
山口　雅敏

＜事務局＞

一般財団法人 医療情報システム開発センター
医療情報安全管理部
プライバシーマーク付与認定審査室　理事長　山本　隆一
部長補佐　岡峯　栄子
室長　吉田　健一郎

認定指針の適用範囲

認定指針は、保健医療福祉分野の事業者がプライバシーマークを取得する際の留意点を示しているが、特にことわりがない場合は医療機関を想定して解説している。ただし、保健医療及び介護福祉情報等の個人情報を主として取り扱う事業者であれば、医療機関との連携があること及び医療機関と個人情報の取り扱いに大きな差異はないことから、医療機関以外であっても本指針に従うこととする。

JIS Q 15001 の構成と認定指針の構成について

JIS Q 15001 と、プライバシーマーク制度における審査基準となる附属書Ａ及びその他の附属書についての解説、本認定指針の構成について、ここに記述する。

JIS Q 15001 の構成

○　JIS Q 15001 本文：「ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針の附属書 SL」に対応する規格構成となっている。

○　附属書Ａ（規定）：JIS Q 15001 の要求事項及び改正個人情報保護法等に対応した要求事項。附属書Ａに示す管理策は、必要な管理策の見落としがないことを確実にするために参照するものであり、附属書Ａの管理策を実施すれば本文の要求事項が満足される。

○　附属書Ｂ：附属書Ａの管理策に関する補足（JIS Q 15001 の解説、経済産業分野ガイドライン等を基にした補足及び推奨事項）。附属書Ｂは規定ではなく参考であり、附属書Ａの補足及び推奨事項である。

○　附属書Ｃ：安全管理措置を講じる参考となる管理策集。附属書Ｃは A.3.4.3.2 安全管理措置の理解を助けるための参考情報であり、取り扱う個人情報の個人情報保護リスクに応じて適宜選択して利用することで良い。

※保健医療福祉分野のプライバシーマークにおいては、附属書Ａの管理策及び後述するＣ．最低限のガイドラインの項目を実施することが原則となる。

認定指針の構成

認定指針は JIS Q 15001 の項目番号と項目名ごとに、下記の構成になっている。

Ａ．JIS Q 15001：附属書Ａ（管理策）

JIS Q 15001 の附属書Ａの管理策を原文通りに記載し、四角の枠で囲んでいる。

Ｂ．保健医療福祉分野としての解釈

保健医療福祉分野に JIS Q 15001：附属書Ａの管理策を適用する場合の解釈を記載している。

Ｃ．最低限のガイドライン

最低限実施しなくてはならない方策の指針を記載している。

Ｄ．推奨されるガイドライン

最低限のガイドラインに保健医療福祉分野の実情を配慮し、追加した方が望ましい方策を含めた指針を記載している。

保健医療福祉分野におけるプライバシーマーク取得の概要

保健医療福祉分野の事業者がプライバシーマークを取得するには、JIS Q 15001 に基づき、事業者が保有する個人情報を保護する為の方針、体制、計画、実施、監査及び見直しを含むマネジメントシステムを構築・運用して MEDIS-DC に申請する。具体的な内容は、

医療機関等で取り扱う診療録、処方伝票、検査依頼伝票、検査結果報告書、看護記録、レセプト、介護記録等の個人情報を含む保護対象を特定し、リスク分析を行い、患者や利用者（以下、「患者等」という）から個人情報の取扱いについての同意を取得し、適切な安全管理のもとに同意の範囲内で利用を行う。さらに教育、点検、苦情及び相談窓口の設置及びマネジメントレビューにより継続的運用と是正を行う。こうしたことが適切に運用されるようにルール化する。単に審査の時点で要求された水準を満足していることのみではなく、個人情報保護マネジメントシステムが継続して運用されるか否かも重要な審査ポイントである。なお、認定指針を審査基準として保健医療福祉分野の事業者を対象に審査を実施するのは、MEDIS-DC だけである。

保健医療福祉分野の個人情報保護の意義

1980 年の OECD プライバシー・ガイドラインの採択により、プライバシーの概念はそれまでの「一人にしておかれる権利」から「自己に関する情報の流れを自身でコントロールする権利」となった。従来、医療機関等でプライバシーというと前者で捕らえられることが多く、一人部屋にすべきとか、中待合室で前の患者等の診察内容が聞こえないようにすべき等に注意が行きがちであったが、新しい個人情報保護の概念では、さらに個人情報を患者等の同意に基づいた利用目的に添って活用していくこと、逆に同意の得られない利用目的には利用しないことが要求される。

すなわち、個人情報保護を行うということは、患者等の情報が外部にもれないようにするため、できるかぎり利用しないように消極的に管理することではなく、活用を望む本人のデータは、その同意した利用目的や利用者の範囲が守られるように安全に管理し、同意に基づいた適切な活用を可能にすることである。

こうした個人情報保護のための活動は、医療情報の開示、医療の透明化を支援し、患者等からの信頼を高め、患者等が主体的に診療に参加する、開かれた医療を実現するために、必要であり、かつ重要な活動であると考えられる。

また、個人情報保護法では、第三条で以下の基本理念を示している。

> （基本理念）第三条　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、その適正な取扱いが図られなければならない。

この基本理念は、患者等の個人情報を保護することは、個人情報（データあるいは物）を保護することだけではないことを明確にしている。個人情報を大切に取り扱うということは、その人の人格を尊重することになるのである。逆に、個人情報を粗末に扱うということは、その人の人格を否定することに繋がると考えるべきである。

保健医療福祉分野の事業者は、常にこの基本理念を念頭に、業務を遂行する必要がある。患者等の個人情報を大切に扱うことは、患者等へのサービス向上にも繋がり、それによりさらなる信頼に繋がることを認識すべきである。

1　適用範囲

A．JIS Q 15001 の要求事項（JIS 規格本文）

この規格は、組織が、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、改善するための要求事項について規定する。この規格が規定する要求事項は、種類又は規模を問わず、全ての組織に適用できることを意図している。～以下、JIS 規格本文を参照～

本要求事項については JIS 規格本文を参照することになる。また、保健医療福祉分野においては実習生、ボランティアなど、従業者の範囲が多岐に渡ることから、本認定指針では、別途規定することとする。

JIS Q 15001:2017 からは、本規格の主体が「事業者」から「組織」に変更されたが、プライバシーマークにおいては、従来通り「事業者」単位で付与されるため、法人全体でマネジメントシステムを構築し運用することが前提となる。

また、JIS 規格本文 3.5 で規定されている「トップマネジメント」についても、事業者の代表者を指すことが原則となるため、医療機関等における「トップマネジメント」とは法人の代表者である理事長又は院長であると考えられる。

B．保健医療福祉分野としての解釈

「事業の用に供している」の「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいう。個人の住所録など個人が自己のために個人情報を取り扱っている場合はこの規格の対象外であるが、営利事業のみを対象とするものではない。従って、研究のために学会発表等に患者等の個人情報を利用する場合も対象となる。

JIS Q 15001 では患者等の個人情報だけではなく、それぞれの医療機関等が雇用する個人（以下、「従業者」という）に関する個人情報や採用情報も対象としている。ただし、従業者に関する個人情報の取扱いに関しては、他の業種と大きな違いはないと考えられるので、本ガイドラインにおいては医療機関等に特有な側面、すなわち患者等の個人情報に関する取扱いに焦点を絞って解説する（看護学校等を併設している場合は、その成績情報等を含めた個人情報も管理対象となる）。

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に留意すべきである（A.3.4.3.4 及び A.3.4.5 に関連）。

C．最低限のガイドライン

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。

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）。

2 用語及び定義

A．JIS Q 15001 の要求事項（JIS 規格本文）

この規格で用いる主な用語及び定義は、個人情報保護法による。その他の主な用語及び定義は、次による。 ～以下、JIS 規格本文を参照～

本要求事項については JIS 規格本文を参照することになる。JIS 規格本文では、「要配慮個人情報」、「匿名加工情報」、「個人識別符号」の各用語の定義は個人情報保護法を参照しており、具体的には記載されていないものの、保健医療福祉分野の事業者とは密接に係るものであるため、本認定指針では別途解説する。

B．保健医療福祉分野としての解釈

（1）保健医療福祉分野における個人情報の考え方

カルテ等の診療記録や介護関係記録については、媒体の如何にかかわらず個人情報に該当する。また、検査等の目的で、患者等から血液等の検体を採取した場合、それらは個人情報に該当し、利用目的の特定（A.3.4.2.1）等の対象となる。また、これらの検査結果については、カルテ等と同様に検索可能な状態として保存されることから、保有個人データ（A.3.4.4.1）に該当し、開示（A.3.4.4.5）の対象となる。個人情報には診療録等の文書情報のみならず、医師と患者、医師と看護師、等の間で交わされる患者等に関する会話、病床における名前の表示、点滴、薬袋などへの名前の表示等も含まれる。これらの個人情報は保有個人データ（A.3.4.4.1）には当たらないが、プライバシーを配慮した取扱いが求められる。

（2）要配慮個人情報

改正個人情報保護法では、要配慮個人情報が新設された。「要配慮個人情報」とは、不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして「個人情報保護法」第 2 条第 3 項、「個人情報の保護に関する法律施行令」第 2 条及び「個人情報の保護に関する法律施行規則」第 5 条で定める記述等が含まれる個人情報をいう。改正個人情報保護法において、要配慮個人情報については、本人に対する不当な差別又は偏見

が生じないように、本人同意を得て取得することが原則義務化された。

医療機関等で想定される要配慮個人情報とは、診療記録や介護関係記録に記載された病歴、診療や調剤の過程での患者等の身体状況、病状、治療などについて医療従事者が知り得た診療情報、健康診断の結果および保健指導の内容、障害の事実、犯罪により害を被った事実などが該当する。

要配慮個人情報の取り扱いにおけるポイントとしては、“患者等の同意を得ずに取得できない”、“オプトアウト（明確に拒否しない限り、同意したと見なすこと）による第三者提供ができない”ことが挙げられる。ただし、当該患者等の医療に必須な利用や、医療機関等の業務に必要な利用は、医療機関等で診療等を受けるということは、診療等を受けることに同意している、つまり医療等を実施するために必要な情報利用にも同意をしているということとなり、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」においても、“患者等に適切な医療サービスを提供する目的のために、当該医療機関等において通常必要と考えられる個人情報の利用範囲を施設内への掲示により明らかにしておき、患者側から特段明確な反対・留保の意思表示がない場合には、これらの範囲内での個人情報の利用について同意が得られているものと考えられる”としている。しかし、JIS 及び本認定指針においては、要配慮個人情報を取得、利用又は提供する場合は、A.3.4.2.3 に基づきあらかじめ書面による本人の同意が原則であることに注意する必要がある。

なお、付録２６に、本認定指針の適用範囲となる「要配慮個人情報」の定義として、「個人情報保護法」第２条 第３項、「個人情報の保護に関する法律施行令」第２条、「個人情報の保護に関する法律施行規則第５条」及び、「個人情報保護法ガイドライン（通則編）」2-3 で定義されている「要配慮個人情報」について記載する。

（３）個人情報の匿名化について

匿名化とは、当該個人情報から、当該情報に含まれる氏名、生年月日、住所、個人識別符号等、個人を識別する情報を取り除くことで、特定の個人を識別できないようにすることをいう。顔写真については、一般的には目の部分にマスキングすることで特定の個人を識別できないと考えられる。なお、必要な場合には、その人と関わりのない符号又は番号を付すこともある。

このような処理を行っても、事業者内で医療・介護関係個人情報を利用する場合は、事業者内で得られる他の情報や匿名化に際して付された符号又は番号と個人情報との対応表等と照合することで特定の患者・利用者等が識別されることも考えられる。法においては、「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」についても個人情報に含まれるものとされており、匿名化に当たっては、当該情報の利用目的や利用者等を勘案した処理を行う必要があり、あわせて、本人の同意を得るなどの対応も考慮する必要がある。

また、特定の患者・利用者の症例や事例を学会で発表したり、学会誌で報告したりする場合等は、氏名、生年月日、住所、個人識別符号等を消去することで匿名化されると考えられ

るが、症例や事例により十分な匿名化が困難な場合は、本人の同意が必要である。

なお、このような学会での発表等のために用いられる特定の患者の症例等の匿名化は、匿名加工情報とは定義や取扱いのルールが異なるので留意が必要である。

※医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスより抜粋

（４）匿名加工情報について

「匿名加工情報」とは、個人情報を個人情報の区分（個人情報保護法第２条第９項参照）に応じて定められた措置を講じて特定の個人を識別することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものをいう。個人情報から匿名加工情報を作成する場合には、個人情報保護委員会規則で定める基準に従って加工する等一定の制限を受けることとなる。

※医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスより抜粋）

なお、本認定指針における匿名加工情報の考え方については A.3.4.2.9 に示す。

（５）個人識別符号

個人識別符号とは、個人の身体の一部の特徴をコンピュータなどで利用する際に変換した符号（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋などの生体情報）のうち、特定の個人を識別するに足りるものとして規則で定める基準に適合するものである。また、旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバーなどの公的機関が割り振る番号なども該当する。

保健医療福祉分野においては、例えば細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列、健康保険法や介護保険法に基づく被保険者証や高齢受給者証の記号、番号及び保険者番号などがある。また、将来的な展望として、医療等（医療、健康、介護）分野の情報に個人番号を付与する「医療等 ID」がある。これに関しては患者が複数の医療機関等で保健医療福祉サービスを受ける際の医療情報連携を円滑にするために、医療等（医療、健康、介護）分野の情報に個人番号を付与するもので、導入に向けて議論が重ねられている（平成 30 年４月現在）。

D．推奨されるガイドライン

保健医療福祉分野のプライバシーマークにおいては、「要配慮個人情報」、「匿名加工情報」、「個人識別符号」は密接な関わりをもつことから、これらについて PMS で別途定義しておくことが望ましい。

Ａ．３．管理目的及び管理策

Ａ．３．１．一般

Ａ．３．１．１．一般

Ａ．JIS Q 15001：附属書Ａ（管理策）

この管理策に規定する A.3.2 から A.3.8 は、トップマネジメントによって権限を与えられた者によって、組織が定めた手段に従って承認されなければならない。

Ｂ．保健医療福祉分野としての解釈

本管理策の考え方について、JIS Q 15001:2017 附属書Ｂでは次のように補足説明している。「“トップマネジメントによって権限を与えられた者”とは、原則として個人情報保護管理者を指す。ただし、承認する案件の軽重は、経営判断を要するものから現場の担当者に任せるものまで様々であり、個人情報保護管理者以外のものが承認する場合もあり得る。

“組織が定めた手段”についても、承認する案件の軽重によって、経営層の決議を要するものから部署内の決済まで様々であると考えられる。」

保健医療福祉分野においては、患者等の要配慮個人情報を取り扱うため、特に適正な取り扱いの厳格な実施を確保する必要があることから、A.3.2 から A.3.8 の管理策（A.3.4.2.3～A.3.4.2.8.3、A.3.4.4.1、A.3.4.4.4、A.3.4.4.5、A.3.4.4.7 のただし書きを適用する事例も含む）で承認が必要な案件についての承認者は、保健医療福祉分野としての特殊性を勘案したうえで決めておく必要があると考えるべきである。

また、「JIS Q 15001:2017 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン」においては、A.3.2 から A.3.8 の管理策毎に個別の承認手順は必須とされておらず、個別の承認手順を設けるか否かは事業者毎の判断によるとしており、本認定指針においても、管理策毎の個別の承認手順を必須とするものではない。

Ｃ．最低限のガイドライン

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）。

Ａ．３．２．個人情報保護方針

Ａ．JIS Q 15001：附属書Ａ（管理策）

A.3.2.1　内部向け個人情報保護方針 トップマネジメントは、5.2.1e)に規定する内部向け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なければならない。 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並びに是正に関すること。 d) 苦情対応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) トップマネジメントの氏名 トップマネジメントは、内部向け個人情報保護方針を文書化した情報を、組織内に伝達し、必要に応じて、利害関係者が入手可能にするための措置を講じなければならない。
A.3.2.2　外部向け個人情報保護方針 トップマネジメントは、外部向け個人情報保護方針を文書化した情報には、A.3.2.1に規定する内部向け個人情報保護方針の事項に加えて、次の事項も明記しなければならない。 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合わせ先 トップマネジメントは、外部向け個人情報保護方針を文書化した情報について、一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。

B．保健医療福祉分野としての解釈

個人情報保護に関する事業者としての考え方や取り組みに関する宣言が「個人情報保護方針」である。医療機関等において、法を遵守し、個人情報保護のため積極的に取り組んでいる姿勢を対外的に明らかにすることが必要である。当然ながら、個人情報保護の理念及び経営責任等を明確にするため、幹部会や運営会議等の決議を経るなど一定の手続を経て定める必要がある。

C．最低限のガイドライン

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。

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。

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。

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。

D．推奨されるガイドライン

当該方針（内部向け・外部向け）には、a）～f）の各事項の文言をそのまま記載するのではなく、a）～f）の各事項に関する保健医療福祉分野の事業者としての特徴をふまえた内容を具体的に記載するとともに、患者等が一読して理解できる簡潔な文章であることが望ましい。

A．３．３　計画

A．３．３．１　個人情報の特定

A．JIS Q 15001：附属書A（管理策）

組織は、自らの事業の用に供している全ての個人情報を特定するための手順を確立し、かつ、維持しなければならない。

組織は、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、利用期限、保管期限などを記載した、個人情報を管理するための台帳を整備するとともに、当該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るようにしなければならない。

組織は、特定した個人情報については、個人データと同様に取り扱わなければならない。

B．保健医療福祉分野としての解釈

（1）保護すべき個人情報の対象及び管理単位

個人情報を特定し管理する単位は、管理が有効に働くレベルである必要がある。一般的には、ファイル単位、帳票名単位、情報システム単位等のレベルでの特定及び管理が良いと思われる。例えば、個人情報管理台帳などによる特定及び管理が考えられる。管理台帳の管理

項目としては、個人情報の名称・個人情報の項目・種類・件数・利用目的・取得方法・情報媒体・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・保管期限などがある。

なお、JIS Q 15001 附属書Ａでは台帳に記載する項目として“件数”及び“委託や提供の有無”は特に明記されていないが、保健医療福祉分野においては、患者等の要配慮個人情報を取り扱うこととなり、取り扱う情報の量による移送・保管等でリスク及びリスク対策が異なっていること、また、委託や提供が発生する際の移送方法等のリスク及びリスク対策が異なっていることから、管理台帳等で項目として管理する必要がある。

※　件数については、事業者内での個人情報の取り扱い状況を把握するためのものであるので、概数でよい。

（２）日常業務としての個人業務の特定手順

個人情報を管理するためには、取り扱う全ての個人情報について洗い出しをしておく必要がある。認識されていない個人情報は、紛失あるいは、改ざんされたとしても、検知することが困難だからである。また、取り扱う個人情報は経営環境等により変化するため、全ての個人情報を日々の業務活動の中で、漏れなく特定できる手順や仕組みを確立しておく必要がある。

（３）個人情報の範囲

プライバシーマーク制度は、個人情報の取扱いについて JIS　Q　15001 に準拠したマネジメントシステムが構築されていることを審査するものである。管理する対象は個人情報となる。従って、そもそも守らなければならない個人情報をどこまでとするかという、個人情報の定義・範囲が重要となる。プライバシー（個人情報）の侵害は人それぞれに考え方の相違があり、一義的に定義することは困難である。よって、個人情報の定義については十分議論し定義する必要があり、特に医療機関等においては要配慮個人情報を事業者全体で取り扱うことを鑑みると、本ガイドラインでは広範な観点で個人情報を捉えておくものとする。

（４）保管期限

個人情報を永久保管とすることは、適切な管理がされなくなる恐れがあり、リスク回避の面から不適切である。特定した全ての個人情報に保管期限を定め、を経過した個人情報を確実に廃棄するか、少なくとも所在を確認して、今後も保管が必要なら、さらに保管を継続する等の対応が必要である。

Ｃ．最低限のガイドライン

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。

→付録4　個人情報取扱申請書の様式例

→付録17　調剤薬局における個人情報管理台帳の例

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）

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。

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。

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。

D．推奨されるガイドライン

医療機関等においては取り扱う個人情報が部署ごとに異なるというよりは、一人の患者等に関連して診療情報等を部署間で共有している場合が多い。従って、個人情報を特定、管理するに当たっては、部署毎で行うというよりは医療系（看護系含む）、事務系などで各々責任者等を定め、その責任者を中心としてマネジメントシステムの開始時、新たな業務の発生時及び不要となった個人情報の確認を定期的に行うことが望ましい。また、責任者以外の従業者も特定作業に漏れがないか意識させることも重要である。

A．３．３．２　法令、国が定める指針その他の規範

A．JIS Q 15001：附属書A（管理策）

組織は、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（以下、“法令等”という。）を特定し参照できる手順を確立し、かつ、維持しなければならない。

B．保健医療福祉分野としての解釈

個人情報に関する法令、国が定める指針及びその他の規範を調査収集し、従業者がいつでも参照できるようにする必要がある。特に、守秘義務を定めた法律がある職種については、

これらを参照可能にしておくこと。

医療機関における個人情報保護に関連する法令条文及び規範などを付録１に示す。また、保健医療福祉分野の事業者は、事業内容（委託も含む）を鑑み、以下の法令、国が定める指針その他の規範等を特定し、参照・維持すること。**→付録5　法令等一覧表の例**

1. 個人情報保護マネジメントシステム－要求事項（JIS Q 15001）
2. 保健医療福祉分野のプライバシーマーク認定指針
3. 個人情報の保護に関する法律
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（第三者提供時の確認・記録義務編）
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（外国にある第三者への提供編）
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（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
9. 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス
10. 医療情報システムの安全管理に関するガイドライン
11. 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
12. 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
13. 診療情報の提供等に関する指針
14. 医療分野の研究開発に資するための匿名加工医療情報に関する法律
15. 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
16. 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）
17. 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（C③に該当する場合）

C．最低限のガイドライン

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。

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。

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。

A．３．３．３　リスクアセスメント及びリスク対策

A．JIS Q 15001：附属書A（管理策）

組織は、A.3.3.1 によって特定した個人情報について、利用目的の達成に必要な範囲を超えた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、維持しなければならない。 組織は、A.3.3.1 によって特定した個人情報について、その取扱いの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確立し、かつ、維持しなければならない。 組織は、現状で実施し得る対策を講じた上で、未対応部分を残留リスクとして把握し、管理しなければならない。 組織は、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、適宜に見直さなければならない。

B．保健医療福祉分野としての解釈

個人情報に関する「原因系リスク」として、不正アクセス、紛失、破壊、改ざん、漏えいなどが代表的である。この原因系リスクが発生した場合の「影響リスク」として、原因究明中の業務中断による損失、患者等に対する賠償などの直接的影響及び、社会的信用の喪失や官公庁への報告、報道機関への公表、訴訟への対応など間接的影響などが考えられる。「リスクを認識する」とは、特定した個人情報の取扱いの一連の流れ（取得・利用・廃棄）に至る各局面において、想定されるリスクを洗い出すことである。また「リスクを分析する」とは、洗い出したリスクに対する現状の対策を評価することである。

リスクは技術の進展や環境の変化等により常に変動するものであり、リスクの認識・分析及び対策は、一度だけ実施すれば良いものではない。医療機関等は、講じた対策が十分であるかを常に検証し見直す姿勢が必要である。

（１）リスク顕在化の予防と発生時対策

対策は一つの方法のみで十分というわけではなく、総合的な検討が求められる。特に安全性の確保に対する対策は漫然と実施するのではなく、A.3.3.1で特定した個人情報を施設の部門別に特定し、その部門での取得、移送、利用、保管、委託・提供、返却・廃棄の各場面で、リスクすなわち脅威と脆弱性を明確に評価する。そして、そのリスクに対するさまざまな予防措置を検討し、その中で医療機関等が取り得る最良の措置を講じることに

より、そのリスクの顕在化を防止する。脅威としては、故意及び過失や災害等が考えられる。また、内部や外部からのものが考えられる。さらに予防対策を行ったにもかかわらずリスクが顕在化した場合の是正措置も必要である。この場合、顕在化を誰がどのレベルでチェックし、誰に連絡し、誰が対策を行うのか等、責任体制の確立が重要である。これにより、リスクが発生しても最低限の損失に止めることができる。

（2）リスク発生時の是正措置

予防措置を講じていたにもかかわらず、個人情報に対するリスクが顕在化する場合も、可能性としては残されている。そのため、是正措置も予め検討して講じる必要がある。是正措置についても、医療機関等が取り得る最善の方法を検討しておかなければならない。なお、是正のための技術的な措置は、前述の予防措置の検討に包含される場合が多く、例えば、アクセスログの取得、バックアップの作成等はこれに当たる。また、漏えい等が起こったときの患者等への対応、関係機関、マスコミ等への対応等の規定（A.3.3.7）も必要である。

（3）プライバシーの観点での分析

医療機関等ではプライバシーの観点での分析も必要である。患者等の呼び出し、病室の名前の表示、お見舞い対応など現状の取扱いを把握し、有用性と保護のバランスの上に適切な対応を実施すること。

（4）残留リスク

すべてのリスクをゼロにすることは不可能であるから、現状で取り得る対策を講じた上で、不十分な点を把握し（残留リスク）、認識する必要がある。現状の対応が十分でないことを認識しながら日常業務に臨むのと、そうでないのとでは結果は大きく異なると理解すべきである。残留リスクの例では、紛失・盗難のリスク対応のため、個人情報を施錠保管するとした場合、残留リスクとして施錠忘れが存在する。その際の残留リスク低減措置として、“A.3.7.パフォーマンス評価”、において、最終退出時の施錠の確認を規定し、実施するなどが考えられる。

C．最低限のガイドライン

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）。

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立すること。

→付録18　調剤薬局における業務フロー兼リスク分析表の例

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。

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。

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。

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。

A．３．３．４　資源、役割、責任及び権限

A．JIS Q 15001：附属書A（管理策）

トップマネジメントは、少なくとも、次の責任及び権限を割り当てなければならない。

a) 個人情報保護管理者

b) 個人情報保護監査責任者

トップマネジメントは、この規格の内容を理解し実践する能力のある個人情報保護管理者を組織内部に属する者の中から指名し、個人情報保護マネジメントシステム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、 業務を行わせなければならない。

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しなければならない。

トップマネジメントは、公平、かつ、客観的な立場にある個人情報保護監査責任者を組織内部に属する者の中から指名し、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、業務を行わせなければならない。

個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、トップマネジメントに報告しなければならない。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。

個人情報保護監査者と個人情報保護管理者とは異なる者でなければならない。

B．保健医療福祉分野としての解釈

医療機関等は、個人情報の適正な取扱いを推進し、漏えい等の問題に対処する体制を整備することが求められている。このため、個人情報の取扱いに関し、専門性と指導性を有し、医療機関等の全体を統括する組織体制・責任体制を構築し、規則の策定や安全管理措置の計画立案等を効果的に実施できる体制を構築する必要がある。

（１）個人情報保護管理者

医療機関等におけるトップマネジメントは法人の代表者である理事長又は院長であると考えられる。トップマネジメントは内部から個人情報保護管理者を定めなければならない。個人情報保護管理者は個人情報保護に対して十分な理解を持つ必要があり、法令で守秘義務が定められている職種の従業者などから選任すべきである。

個人情報保護管理者は専任である必要はないが、個人情報保護に関する権限と責任を与えられなければならない。例えば内科医局員の一人を個人情報保護管理者に選任した場合、個人情報保護に関する権限や責任は医局長や内科部長の干渉をうけないことを定める必要がある。そして個人情報保護管理者とその権限及び責任をすべての従業者に周知しなければならない。

（２）個人情報保護監査責任者

トップマネジメントは、内部から個人情報保護監査責任者を定めなければならない。個人情報保護監査責任者は「公平、かつ、客観的な立場」にあることが求められていることから、個人情報保護管理者との兼任は許されない。また、個人情報保護管理者を牽制する立場であることから、個人情報保護管理者の直接の指揮命令下にないものが望ましい。医療機関等においては看護師長クラス以上が適当と考えられる。

医療機関等の内部で監査の独立性と公平性が確保できない等の場合は、監査の実務を外部に委託することも可能であるが、個人情報保護監査責任者は必ず内部から選任すること。

（３）個人情報保護に必要な資源

トップマネジメントは、個人情報保護に必要な資源を用意しなければならない。資源とは、人員、組織の基盤（規程、体制、施設・設備等）や資金などを意味するが、事業者の状況に応じて、適宜、必要な資源を判断し、用意することが求められる。

（４）倫理委員会の設置

医療機関等における個人情報保護は微妙な問題が数多く存在する。このような問題に対処するために可能であれば外部の有識者を含めた倫理委員会を設けるとよいであろう。個人情報保護だけでなく医療には診療上の必要性と倫理に微妙な問題が多く、そのような場面でも倫理委員会は重要である。臓器移植法やヒトゲノムの臨床研究のガイドラインなど、倫理委員会の存在や構成が指定されている法律・規範があるので、倫理委員会を構成する場合は参照することが望まれる。また診療所などの小規模な医療機関等では単独で倫理委員会を設けるのは困難であるが、例えば地区医師会などで設けるなどの工夫が推奨される。

Ｃ．最低限のガイドライン

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。→付録6　医療機関における個人情報保護体制図の例

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。

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。

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。

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）。

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。

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。

D．推奨されるガイドライン

① 個人情報保護管理者は、法令で守秘義務が定められている職種の従業者から選任し、医療機関等における個人情報の取扱いに関する安全管理面だけではなく、医療機関等の運営に関する全体の情報管理職であることが望ましい（例えば、副院長クラス）。

② 個人情報保護と医療等の必要性との間で問題が生じた場合には、外部の学識経験者を含めた倫理委員会にて審議すること。倫理委員会については本ガイドライン以外にも臓器移植、ヒトゲノムの取扱い、疫学研究などに関してのガイドライン等で規定されている。本ガイドラインでは外部の学識経験者を含める以外に特に構成等を規定しないが、他のガイドラインに関係する医療機関等にあってはそれぞれのガイドラインでの倫理委員会の規程を満たす必要がある。また他のガイドラインに従って構成された倫理委員会であっても、外部の学識経験者が含まれている限り、本ガイドラインで規定する倫理委員会とみなしてよい。

③ 情報システムの管理者特権を持つ担当者の過失や故意による事故を防止するため、複数の担当者を選任し交代で担当することが望ましい。

④ 医療機関等において、複数の拠点がある場合（特に拠点毎に異なる情報システムを導入している場合など）は、拠点間の連携を密に行ない、情報システムの安全管理措置についてのレベルの均一化を図るため、拠点毎に情報システム担当者（副）を選任することが望ましい。

⑤ 個人情報保護対策及び情報セキュリティ対策に十分な知見を有する者（必要に応じ外部の者を活用することを含む）による監査実施体制を整備することが望ましい。

Ａ．３．３．５　内部規程

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、次の事項を含む内部規程を文書化し、かつ、維持しなければならない。

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) 個人情報保護リスクアセスメント及びリスク対策の手順に関する規定
d) 組織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など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

組織は、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しなければならない。

Ｂ．保健医療福祉分野としての解釈

本管理策は、内部規定に定めるべき最低限の事項を例示したものである。内部規程には、マネジメントシステムの中核をなす基本規程、及び従業者が組織として統一的、合理的に行動し得るよう細則、様式などから構成される。この基本規程及び細則等の文書を包括して内部規程という。内部規程は、従業者に対し十分に教育し周知がなされなければならない。従業者が遵守すべきルールは、できるかぎり明文化することが重要である。ルールを内部規程として明文化されていないと、ルールから逸脱した取り扱いがあっても違反に問えないことを認識すべきである。

Ｃ．最低限のガイドライン

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。
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。
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。

A．３．３．６　計画策定

A．JIS Q 15001：附属書A（管理策）

組織は、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、少なくとも年一回、次の事項を含めて、必要な計画を立案し、文書化し、かつ、維持しなければならない。 a）A.3.4.5 に規定する事項を踏まえた教育実施計画の立案及びその文書化 b）A.3.7.2 に規定する事項を踏まえた内部監査実施計画及びその文書化

B．保健医療福祉分野としての解釈

（１）計画書の作成

個人情報を保護するためには、従業者に内部規程を遵守して行動させるための教育が不可欠である。また、内部規程どおりに運用を実施しているかをチェックするための監査が必要である。教育や監査などを効果的かつ効率的に実施するためには、計画書を策定することが求められる。計画書を策定するためには、担当部署（担当者）が計画書を立案し、承認を得る必要がある。

なお、教育、監査計画書以外に、どのような計画書を作成するかは、PDCA サイクルの C（点検）や A（見直し）で把握された課題もふまえ、事業者の置かれた状況等を勘案し、個別に必要性を検討することが望ましい。例えば、中長期的な視点もふまえた安全管理（情報セキュリティ対策）計画書などが考えられる。

計画書は、教育や監査等の個別の規定の中で、計画項目を定めておくか、書式を定めておき、その内容を埋めることで必要な項目が充当されるような仕組みを取る必要がある。

a）教育計画書に必要な項目→付録7　教育基本計画書の様式例

年間カリキュラム（テーマ、回数、時期、対象、承認欄）

個別の研修プログラム

- 研修の名称
- 研修の目的・概要、使用テキスト
- 開催日時、場所、講師
- 任意参加か否かの別、予算
- 受講対象者及び予定参加者数
- 出欠状況の確認方法、教育効果の確認方法
- 欠席者への対応方法
- 承認欄

b）監査計画書に必要な項目→付録10　監査基本計画書の様式例

年間計画（テーマ、回数、時期、対象、承認欄）

個別計画

- 監査テーマ
- 監査対象、監査員
- 目的、範囲、方法
- スケジュール
- 承認欄

（2）他の計画との統合

これらの教育、監査は従来から医療機関等で行われてきたものと統合して行って良いが、個人情報保護の観点が明確になるようにすること。また、日勤、夜勤、準夜勤など保健医療介護分野特有の勤務体系も配慮し教育計画を立てる必要がある。

C．最低限のガイドライン

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。

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

b） 必要な資源

c） 責任者

d） 達成期限

e） 結果の評価方法

D．推奨されるガイドライン

① 教育計画書は、対象や勤務形態を考慮し、年間カリキュラムと個別の研修プログラムに分けて立案することが望ましい。**→付録8　教育個別計画書の様式例**

② 監査計画書は、対象や部門を考慮し、当該年度に実施する全体スケジュールと個別計画に分けて立案することが望ましい。**→付録11　監査個別計画書の様式例**

A．３．３．７　緊急事態への準備

A．JIS Q 15001：附属書A（管理策）

組織は、緊急事態を特定するための手順、及び、特定した緊急事態にどのように対応するかの手順を確立し、実施し、かつ、維持しなければならない。 組織は、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、維持しなければならない。 また、組織は、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、維持しなければならない。
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、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。

B．保健医療福祉分野としての解釈

個人情報に関する事故は、100% 防ぐことは困難であることを認識し、緊急事態を想定し、対処方法を事前に準備しておくことが必要である。特に、医療機関等では取り扱う個人情報の重要性が高いことから、悪用されると本人への影響が大きいことを認識して緊急事態への準備を行うべきである。

医療機関等は他の事業者と異なり、医療過誤や医療事故に対する対応策を準備している場合が多い。これらの対応策をベースに緊急事態への対応策を策定することが適切であろう。また、1）個人情報の漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合、2）個人情報の取扱いに関する規程等に違反している事実が生じた場合、又は兆候が高いと判断した場合等における内部及び関係機関等への報告連絡体制の整備を行うことは必須である。個人情報の漏えい等の事例は、苦情及び相談等の一環として、外部から報告される場合も想定されることから、苦情及び相談の対応体制との連携も図ることも必要である。

C．最低限のガイドライン

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。
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。
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

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。

D．推奨されるガイドライン

緊急事態は予測なしに発生する場合がほとんどであることから、緊急時対応についての教育訓練に関することも規定し、定期的に実施することが望ましい。

A．３．４　実施及び運用

A．３．４．１　運用手順

A．JIS Q 15001：附属書A（管理策）

組織は、個人情報保護マネジメントシステムを確実に実施するために、運用の手順を明確にしなければならない。

B．保健医療福祉分野としての解釈

医療機関等における個人情報の取り扱いは、診療部門、事務部門など部門により個人情報の種類、取得方法、利用目的、管理方法等の運用手順は異なるはずである。部門別に運用の手順を明確にすることが望ましい。また、確立した運用手順（ルール）を文書化することは、担当者が変わっても一定の個人情報保護水準を維持できることにつながり、文書化されていないことは実施されなくなる可能性がある。従って、文書化していないことは、パフォーマンス評価(A.3.7）から漏れる可能性が大きく、リスクとなることを認識すべきである。

また、個人情報保護マネジメントシステムは、単に個人情報を保護するためのルールを策定すればよいのではなく、それを実現するための組織体制を整え、具体的な計画（Plan）を立て、それを実施（Do）し、その状況を点検、監査（Check）し、運用状況を評価し見直す（Act）必要がある。さらに、その評価に基づき、個人情報を保護するための方針をより確実に実現できるように、計画を練り直すという具合に、このP→D→C→Aを繰り返すことが要求されている。こうした個人情報保護のためのマネジメントシステムは、医療情報の開示の促進や、医療の透明化に寄与することから、患者等からの信頼を高め患者等が主体的に診療に参加する、開かれた医療を実現するために必要であり、かつ重要な活動であると考えられる。

C．最低限のガイドライン

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）。

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

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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わなければならない。 組織は、利用目的の特定に当たっては、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するよう配慮しなければならない。

Ｂ．保健医療福祉分野としての解釈

医療機関等での個人情報の利用目的は、一義的には当該個人すなわち患者等の健康の維持及び回復であるが、そのほかに一般的に以下のものがありうる。このような目的にまったく必要のない情報取得がないことを確認する必要がある。利用目的の特定に当たっては、利用目的を具体的に明確に定めることが必要である。

また、住宅地図のような公開された資料などから個人情報を取得する際においても、組織としての利用目的を特定し、特定した利用目的の範囲内で取り扱う必要がある。

（１）患者等の健康の維持と回復など直接的な利益が目的である場合

- 患者等の診療や説明
- 患者等の家族に対する説明
- 他の医療機関へ患者等を紹介する場合、又は患者の診療にあたって、他の医療機関の医師の意見を照会する場合
- 本人の調剤を現に行っている調剤薬局や本人が受診している他の医療機関からの照会に対しての返答

（２）病院事務あるいは経営上必要な場合

- 診療報酬の請求事務
- 医療機関の経営、運営のための基礎データ
- 医療機関の上部組織への報告
- 医療監視や医療指導監査などへの対応

（３）医療の向上への寄与

- 臨床治験
- 臨床研究
- 医師や看護師、その他の医療従事者の教育や臨床研修

（４）行政上の業務への対応

- がん登録のような公益性の高い疫学調査の実施
- 厚生労働省等の医療行政等にかかわる統計･調査、サーベイランス事業
- 保健所など公的機関に対する保健医療及び公衆衛生上の報告

（５）保険業務への対応

- 労働者災害補償保険や自賠責の手続きなど
- 一般の保険会社等からの問合せ

（6）その他問合せ

- 患者等の職場、学校等に対する情報提供
- 警察からの問合せ
- 裁判所からの問合せ

C．最低限のガイドライン

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）。

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）で利用目的を明確にしている）。

D．推奨されるガイドライン

① マネジメントシステム作成にあたっては、当該医療機関等で過去に診療情報が利用された実績を詳細に調査し、すべて列挙すること。そして利用する情報がこれらの目的にだけ利用されていることを定期的に確認すること。また、いずれの目的にも利用されない情報取得が行われていないか定期的に確認すること。

A．３．４．２．２　適正な取得

A．JIS Q 15001：附属書A（管理策）

組織は、適法かつ公正な手段によって個人情報を取得しなければならない。

B．保健医療福祉分野としての解釈

（1）患者等から個人情報を得る場合、十分な説明を行った上での患者等による自発的な提供を原則とし、強要をしてはいけない。また、診療情報の取得は原則として当該個人から得られるもので、適法かつ公正と考えられる。しかし、次に列挙するものは適法性、公正性に配慮を必要とする。

1）意識障害・精神障害のある患者、乳幼児である患者で、情報を家族から得る場合。

2）意識障害・精神障害のある救急搬送患者で、情報を（家族でない）搬送員又は当該患者の所持物等から得る場合。

3）生活環境に問題がある場合で、近隣の住民及び職場の人等から情報を得る場合。

4）検査等で、対象項目外で偶発的に発見した異常値や、測定上同時に得られてしまう値等。

５）紹介元に検診結果を問い合わせる場合。

６）本人から家族歴等の調査の目的で当該個人以外の情報を取得する場合。

これらの場合でも基本的には医療上の必要性が十分あれば、適法かつ公正と考えることができるが、特に上記の２）の所持物の検査などは、可能な限り警察等にまかせるべきで、医療の遂行上やむをえない場合をのぞいて行ってはならない。また実施する場合は、その必要性を出来る限り速やかに診療録等に記載すること。意識の回復が期待できるが、事務手続きのために名前や住所が必要と言った場合には慎むべきで、緊急に連絡先が必要な場合などに限定することが求められる。

６）に関しては個人情報保護の対象となる個人が当該患者等以外であり、問題を含んでいる。ただ、家族歴は多くの場合医療の遂行上必須であり、また個々に対象個人の同意を得ることは極めて困難であるので、取得することはやむを得ないが、その扱いには十分な配慮が求められる。

なお、個人情報保護法第 23 条に規定する第三者提供制限違反（本人同意なしの個人情報の提供など）がされようとしていることを知り、または容易に知ることができるにもかかわらず、個人情報を取得する場合なども、適正な取得とは認められない。

C．最低限のガイドライン

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）。

② 当該患者等以外の情報を患者等から得る場合は、その情報の必要性を十分検討した後に行い、取得された情報の利用は当該患者等の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。

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。

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。

D．推奨されるガイドライン

C．に加えて患者等に関するもの以外の情報を患者等から得る場合で、対象個人の了承を得られない場合と、患者等以外から当該患者等の情報を得る場合で当該患者等の了承を得ることができない場合は、保健医療福祉サービス遂行の必要性を複数の従業者が検証を行うこと。また、当該個人情報の内容に疑義が生じた場合には、記載内容の事実に関して本人又は情報の提供を行った者に確認をとること。

A．３．４．２．３　要配慮個人情報

A．JIS Q 15001：附属書A（管理策）

組織は、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本人の同意を得ないで、要配慮個人情報を取得してはならない。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

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

組織は、要配慮個人情報の利用又は提供についても、前項と同様に実施しなければならない。さらに、要配慮個人情報のデータの提供についても、同様に実施しなければならない。

B．保健医療福祉分野としての解釈

（１）あらかじめ書面による本人の同意の原則

本管理策は、改正個人情報保護法第 17 条第 2 項において「要配慮個人情報」が新設されたことにより、JIS Q 15001:2017 においても、旧 JIS 規格の「特定な機微な個人情報の取得、利用及び提供の制限」に変わり新設された項目である。本項目は保健医療福祉分野での事業者と、一般の事業者とで最も大きな違いが見られる事項である。要配慮個人情報の取得は、保健医療福祉サービスの提供に際して必須であり、これらの取得なしには事業が成り立たない。従って、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原則とすべきである。あらかじめ書面による本人の同意とは、インフォームド・コンセントに近い概念であり、黙示的な同意は認められない。

また、本認定指針２用語及び定義のＢ．（２）で解説している通り、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」では、当該患者の医療に必須な利用や、医療機関等の業務に必要な利用は、医療機関等で診療等を受けるということは、診療等を受けることに同意している、つまり医療等を実施するために必要な情報利用にも同意をしているということとなり、“患者に適切な医療サービスを提供する目的のために、当該医療機関等において通常必要と考えられる個人情報の利用範囲を施設内への掲示により明

らかにしておき、患者側から特段明確な反対・留保の意思表示がない場合には、これらの範囲内での個人情報の利用について同意が得られているものと考えられる”としているが、JIS 及び本認定指針においては、要配慮個人情報を取得、利用又は提供する場合は、A.3.4.2.3 に基づきあらかじめ書面による本人の同意が原則であることに注意する必要がある。

同意を得ずに要配慮個人情報を取り扱う場合は、本管理策のただし書きａ）～e）に該当することを確認し、診療上の理由が自明でない限り、その理由を診療録等に明記した上で取り扱うこと。その場合も利用は診療上必要な範囲内にあることに特に注意しなければならない。診療上の理由が自明とは、性生活そのものが健康上の問題である場合の性生活に関する情報や、思想、宗教、犯罪歴などが妄想などの精神症状に強く関連している場合であって、安易に本管理策のただし書きａ）～e）に該当すると判断してはいけない。本管理策のただし書きａ）～e）に該当する事例を以下に示す。

ａ）法令に基づく場合

○ 医療法に基づく立入検査、介護保険法に基づく不正受給者に係る市町村への通知、児童虐待の防止等に関する法律に基づく児童虐待に係る通告等、法令に基づいて個人情報を利用する場合

○ 感染症予防法による保健所への報告や児童虐待防止法による報告

○ 警察や検察等の捜査機関の行う刑事訴訟法第１９７条第２項に基づく照会（同法第５０７条に基づく照会も同様）は、相手方に報告すべき義務を課すものと解されている上、警察や検察等の捜査機関の行う任意捜査も、これへの協力は任意であるものの、法令上の具体的な根拠に基づいて行われるものであり、いずれも「法令に基づく場合」に該当すると解されている。

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

○ 意識不明で身元不明の患者について、関係機関へ照会する場合

○ 意識不明の患者の病状や重度の痴呆性の高齢者の状況を家族等に説明する場合

○ 意識不明で身元不明の患者について、関係機関へ照会したり、家族又は関係者等からの安否確認に対して必要な情報提供を行う場合

○ 大規模災害等で医療機関に非常に多数の傷病者が一時に搬送され、家族等からの問い合わせに迅速に対応する場合等で、本人の同意を得るための作業を行うことが著しく不合理である場合

○ 児童・生徒の治療に教職員が付き添ってきた場合についても、児童・生徒本人が教職員の同席を拒まないのであれば、本人と教職員を同席させて、治療内容等について説明を行うことができる

○ 報道機関や地方公共団体等を経由して、身元不明の患者に関する情報が広く提供されることにより、家族等がより早く患者を探しあてることが可能になると判断でき

る場合

○　急病その他の緊急時に、付添者が患者の血液型や家族の連絡先等を医師や看護師等に提供する場合

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

○　健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供

○　がん検診の精度管理のために地方公共団体又は地方公共団体から委託を受けた健診機関に対する精密検査結果の情報提供

○　児童虐待事例についての関係機関との情報交換

○　医療安全の向上のため、院内で発生した医療事故等に関する国、地方公共団体又は第三者機関等への情報提供のうち、氏名等の情報が含まれる場合

○　不登校児童生徒の問題行動について、児童相談所、学校、病院等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

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

○　国等が実施する、統計報告調整法の規定に基づく統計報告の徴集（いわゆる承認統計調査）及び統計法第８条の規定に基づく指定統計以外の統計調査（いわゆる届出統計調査）に協力する場合

○　災害発生時に警察が負傷者の住所、氏名や傷の程度等を照会する場合等、公共の安全と秩序の維持の観点から照会する場合

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

○　当該要配慮個人情報が、本人、国の機関、地方公共団体、個人情報保護法 76 条 1 項各号に掲げる者（例：報道機関が特定の個人の信仰や前科に触れる報道をする場合）、外国政府、外国の政府機関、外国の地方公共団体または国際機関、外国における個人情報保護法 76 条 1 項各号に掲げる者に相当する者により公開されている場合

（2）あらかじめ書面による本人の同意を得られない時

保健医療福祉分野では、人種、民族、身体・精神障害及び保健医療情報だけでなく、思想、信条、犯罪歴でさえも、精神疾患などの治療において必要な場合がある。しかしながら、これらの情報の取得に際しては、あらかじめ書面による本人の同意を得ることが困難な場合がある。同意を得ずにこれらの情報を取得・利用・提供するには、本管理策のただし書き a)～e)に該当することを確認する必要がある。また、これらは特に個人情報保護に敏感な項目であるために挙げられたことに十分注意するべきで、同意なしにこれらの情報を取得する場合は、特に利用範囲が保健医療福祉サービスの遂行のための限度内であることが前提と

なる点にも留意すべきである。

（３）倫理委員会での方針決定

個人情報保護に敏感で医療の遂行上必要な情報は少なからず存在する。これらの情報取得には慎重でなければならないが、複雑な手続きを規定すると保健医療福祉サービスの遂行が困難になることもあり得る。このような情報は診療の専門性によっても異なるために一概に判断することは困難である。その組織の実態をよく把握し、日常的な情報取得で少しでも曖昧さがある場合はあらかじめ倫理委員会で方針を決めるなどの、説明可能な対策が求められる。

（４）宗教に関する取得の事前通知と拒否

特殊な例として、宗教法人が運営する医療機関等などで信者か否かを受診時に確認する場合がある。これも宗教に関する情報取得に当たるが、医療面からの必要性は乏しく、安易に取得すればプライバシーの侵害となる恐れがある。このような場合は、初診申し込み前に宗教に関する質問があることを通知し、回答を拒否できるようにするべきである。またホスピス等で、本人の宗教によってケアが異なる場合のために情報を取得する場合がある。診療上の必要性はあると考えられるが、止むを得ないかどうかは判断が困難である。このような場合にも、事前に通知し、回答を拒否できるようにしておくべきである。

Ｃ．最低限のガイドライン

① 保健医療福祉分野では、要配慮個人情報を主として取り扱うという観点から、個人情報の取得・利用・提供に際しては、あらかじめ書面による本人の同意を得ることが前提となる。

② 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）。

Ｄ．推奨されるガイドライン

同意を得ずに要配慮個人情報を取り扱う場合は、本管理策のただし書き a)～e)に該当することを確認するが、診療上の必要性が自明でない場合、可能な限り事前に倫理委員会の了承を得る。事前に倫理委員会に諮ることが出来なかった場合は、事後に倫理委員会に報告し、その際、不適と判断された場合は当該情報を抹消する。例えば不妊外来での性生活に関する情報取得のように、診療上の必要性があって、かつ日常的に取得されることが予想される場合は、あらかじめ一括して倫理委員会等で検討を行い、必要性を明確にし、個人情報保護上の配慮を具体的に定めておく。このような過程を経た情報取得はその必要性と配慮がある前提で、個々に特別な手続きを経ずに取得することができる。

Ａ．３．４．２．４　個人情報を取得した場合の措置

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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、又は公表しなければならない。ただし、次に掲げるいずれかに該当する場合には、本人への利用目的の通知又は公表を要しない。

a）利用目的を本人に通知するか、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

b）利用目的を本人に通知するか、又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合

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とき

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

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

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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なければならない。

a）組織の名称又は氏名

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）A.3.4.4.4～A.3.4.4.7 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）本人が容易に知覚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

ただし、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、又はただし書き A.3.4.2.4 の a)～d)のいずれかに該当する場合は、本人に明示し、本人の同意を得ることを要しない。

JIQ15001:2006(旧規格)の 3.4.2.4、3.4.2.5 と、JIS Q 15001:2017(新規格)の A.3.4.2.4、A.3.4.2.5 は、構成が以下の様に変更となった。

○　旧規格 3.4.2.4→新規格 A.3.4.2.5

○　旧規格 3.4.2.5→新規格 A.3.4.2.4

新規格では、A.3.4.2.5 に基づき本人から直接書面によって個人情報を取得する場合には、A.3.4.2.4 に定められた対応(利用目的の公表や通知など)を行っていることが前提となっている。また、A.3.4.2.4 と A.3.4.2.5 は密接に関連する管理策であるため、本認定指針においては、一緒に解説する。

B．保健医療福祉分野としての解釈

（1）あらかじめ書面による本人の同意を原則とする

“A.3.4.2.5 の 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”は、本人すなわち患者等から当該患者等に関する情報を直接書面（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）により取得する場合の管理策であり、それぞれ情報取得を行う前に患者等に明示し（口頭による説明は含まれない）、同意を得る必要がある。

一方、“A.3.4.2.4 個人情報を取得した場合の措置”は、委託を受けた場合、第三者として提供を受けた場合、公開情報から取得した場合等、本人から直接書面により取得する場合以外は、この管理策が適用される。つまり本人から直接取得しているが書面で取得しなかった場合（監視カメラによる取得、口頭による取得等）も含まれることとなる。

しかし、保健医療福祉分野では、患者等から直接書面により個人情報を取得する場合より、口頭（問診等）や第三者（家族等）からだけでなく、血液等の検体、X線フィルム等の画像からも個人情報を取得する事例がある。さらに、取得・利用・提供する個人情報のほとんどが“A.3.4.2.3 要配慮個人情報”に該当する個人情報である。従って、保健医療福祉分野における個人情報の取得は、A.3.4.2.4 及び A.3.4.2.5 を適用するのではなく、A.3.4.2.4 に該当する場合でも、A.3.4.2.3 に基づき A.3.4.2.5 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べきである。

（2）患者等本人以外からの取得

以上のことから、患者等の家族、職場や近隣の人々、紹介元、ケースワーカー、ソーシャルワーカー、ケアマネージャー、介護福祉士、ヘルパー、搬送を担当した救急隊員、警察等から情報を得る場合等、本人以外から個人情報を取得する際も原則として当該患者等に通知の上で同意を得る必要がある。しかし保健医療福祉の現場では種々の事情で本人から同

意を得ることが難しいことがある。意識障害がある場合や、本人が虚偽を述べている場合などがこれに当たる。このような場合は保健医療福祉サービスの遂行上の必要性が重要で、これを確認して行わなければならない。

（３）患者等本人に理解能力がない場合の同意

乳幼児や意識障害、精神障害で本人に理解する能力がない場合は、可能な限り親権者や保護者の了解又は同意を得る必要がある。ただし乳幼児及び小児で親権者による虐待の可能性がある場合は、その親権者の同意や了解は必要ない。この場合は当然、法律に基づいて虐待の可能性を報告しなければいけない。

親権者や保護者が複数いて、意見に相違がある場合は原則として不同意を優先する。ただし、患者等や第三者の人命にかかわる場合や、身体に重大な損傷をあたえることが予想される場合は同意を優先してよい。その場合、優先した理由を速やかに診療録等に記載すること。

（４）包括的同意と個別同意

個別同意とは、個人情報の利用を行う都度、事前に利用目的等を明示し、本人の同意を得ることである。包括的同意とは、患者等の個別の状態によらず、予想される利用目的等を列挙並びに明示し、同意を得ることである。

JIS Q 15001 の要求は、項目毎の個別の同意か、包括的な同意かについて言及はしていない。医療機関等の健全な運営も含めて保健医療福祉サービスの遂行上必要な目的に関しては、包括的な同意でよいと考えられるが、教育・研修や医学研究といった保健医療福祉サービス遂行上の必要性が薄い項目に関しては、利用時に個別に同意を得るべきである。

直接診療に用いる場合や、診療報酬請求や病棟管理などの医療機関等の経営や管理上の利用は、本来目的であり包括的な同意でよいと考えられる。しかし、お見舞い客の案内に用いる入院名簿に掲載するといった利用目的は、利用できなくても診療にも病院の経営・管理にも重大な障害とはならない。このような目的は、患者等に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。**→付録２２　医療機関における同意文書の例**

（５）同意を得られない場合の措置

患者等が意識障害・精神障害・乳幼児等で本人の同意が得ることができない場合、保健医療福祉サービスの遂行上の必要性を十分検討し、その必要性を診療録等に記載した上で情報の取得を行うこと。緊急事態等で事前の記載が不可能な場合は、可及的速やかに事後に記載すること。また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の同意を得ること。ただし患者等が乳幼児又は小児等で親権者による虐待が疑われる場合は、その親権者の同意は必要ない。

（６）利用目的の公表

医療機関等においても、A.3.4.2.4 に該当する事例も必ず存在することから、利用目的を広く公表することが求められる。利用目的等を広く公表することについては、医療機関等で個人情報が利用される意義について患者等の理解を得るという趣旨であり、これにより同意が得られていると判断してはならない。また、委託された場合（検体検査の受託、遠隔画

像診断の受託等）であっても、A.3.4.2.4 のただし書きｄ）には該当せず、その利用目的を本人に通知又は公表しなければならない。利用目的の公表方法としては、院内や事業所内等に掲示するとともに、可能な場合にはホームページへの掲載等の方法により、なるべく広く公表する必要がある。

A.3.4.2.4 のただし書きｃ）の事例としては、公開手配を行わないで、被疑者に関する情報を、警察から被疑者の立ち回りが予想される医療機関等に限って提供された場合、医療機関等が利用目的を本人に通知し又は公表することにより、捜査活動に重大な支障を及ぼす恐れがある場合などが該当する。

利用目的の公表に当たっては、診療に関して患者情報を用いるのは当然との意識があるが、どこまでが診療か、どこまでが病院管理かなど、明確な定義が出来ない場合もある。そのため、患者等の個人情報が何に利用されているのかを具体的に示しておくのが望ましい。例えば、「ご家族への病状説明に利用します」、「診療報酬の請求に利用します」など、これまで暗黙の内に当然の利用目的としていたものに関しても、明文化しておけば、患者等の理解をより得やすくなるであろう。

→付録23　医療機関における個人情報の利用目的の例

Ｃ．最低限のガイドライン

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。

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。

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。

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。

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。

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）。

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）。

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。

- 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）。

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。**→付録22　医療機関における同意文書の例**

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。

D．推奨されるガイドライン

緊急時等で事前に同意を得ることができなかった場合や、個人情報の取り扱いについて十分な理解ができない患者等も想定されることから、患者等が落ち着いた時期に改めて説明を行ったり、診療計画書、療養生活の手引き等の保健医療福祉サービス提供に係る計画書等に個人情報に関する取扱い方法を記載したりするなど、患者等が個人情報の利用目的を理解できるよう配慮することが望ましい。

A．３．４．２．６ 利用に関する措置

A．JIS Q 15001：附属書A（管理策）

組織は、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しなければならない。 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には、本人の同意を得ることを要しない。

B．保健医療福祉分野としての解釈

診療情報の利用を原則としてあらかじめ同意を得た範囲に限定するものである。ただし、本人が虚偽を申し立てている可能性が強い場合で、保健医療福祉サービスの遂行上の必要性が高い情報である場合も本人の同意なく情報を取得し利用することができるが、本人が虚偽を申し立てていると判断した理由及びその情報が保健医療福祉サービスの遂行上必要である理由を診療録等に記載することが必要。

なお、A.3.4.2.3 のただし書きａ）～ｄ）に基づき、本人の同意を得る必要はない事例については、A.3.4.2.3 に示す。

C．最低限のガイドライン

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。

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。

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。

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）。

D．推奨されるガイドライン

① 法令による利用であってもその利用を通知しておくことが望ましい。

② 学会発表等で匿名化して利用する場合であっても、事前に本措置に則ったあらかじめ書面による本人の同意を得ることが望ましい。

③ 緊急避難的利用の場合も、事後にその利用を通知しておくことが望ましい。

A．３．４．２．７　本人に連絡又は接触する場合の措置

A．JIS Q 15001：附属書A（管理策）

組織は、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、本人の同意を得なければならない。ただし、次に掲げる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、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 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) 個人情報を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
- 取得方法

e) A.3.4.2.4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) 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

B．保健医療福祉分野としての解釈

（1）あらかじめ書面による本人の同意を原則とする

個人情報を本人から直接取得せずに、公開情報や第三者から取得し、本人に対して電話、郵便、メールなどを送ること又は訪問することにより連絡又は接触する場合の措置である。医療機関等では、入院時等に患者等から第三者（家族・親類等）の連絡先を記入してもらい（A.3.4.2.5 以外による取得）、これにより患者等の健康状態等を家族や親類等に問い合わせる場合等（本人に連絡又は接触）が想定される。

また、ただし書きに該当する事例としては、b）健診業務の委託、介護相談窓口の委託など、c）医療機関等の事業の継承など、d）地域間、施設間等での医療・介護情報等の連携等による共同利用が想定される。

（2）共同利用について

共同利用により本人に連絡又は接触する場合は、共同利用者（連携元）が、本人から個人情報を取得する際に、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ことが前提である。さらに、共同利用者（連携先）は、d）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、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。“共同して利用する者の範囲”は、本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要でない場合もある。例えば、最新の共同利用者のリストを本人が容易に知り得る状態に置いているときなどが該当する。

なお、共同利用を実施する際には共同利用する者の間で、A.3.4.2.8のC⑦で求められている項目を契約書等で定めておく他、以下の事項などを取り決めておくことが望ましい。

- 共同利用者の要件

- 各共同利用者の個人情報取扱責任者・問い合わせ担当者及び連絡先
- 共同利用する個人データの取扱いに関する事項（漏えい防止に関する事項、目的外加工、利用、複写、複製等の禁止など）
- 共同利用する個人情報の取扱いに関する取り決めが遵守されなかった場合の措置
- 共同利用する個人情報に関する事件・事故が発生した場合の報告・連絡に関する事項
- 共同利用を終了する際の手続

（3）委託される場合

個人情報の取り扱いを委託される場合は、本管理策のただし書きｂ）に該当し、本人からの同意を不要とされている。しかし、健診業務やストレスチェック業務の委託のように保健医療情報という要配慮個人情報を取り扱うこと及び本人と直接面談や、通知文書の同封等により本人の同意意思を確認する機会があることから、あらかじめ書面による本人の同意を得ること。労働安全衛生法に基づく健診を委託された場合であっても、委託された事業者から見ればA.3.4.2.3のただし書きａ）には該当せず、また、ｄ）にも該当しない（学童検診は除く）と理解すべきである。

（4）あらかじめ書面による本人の同意を得る方法

健診業務やストレスチェック業務等を委託された場合のあらかじめ書面による本人の同意を得る方法としては、1）受診票あるいは別紙にA.3.4.2.5で規定された事項を明示し、受診票の同意欄あるいは不同意欄にチェックしてもらう。（ストレスチェックのように、本人と直接面談する機会がない場合は、少なくとも“同意のうえ送付ください”などの文言を記載しておく）2）受診案内の際など、事前にA.3.4.2.5で規定された内容の文書を郵送等で明示し、内容について同意の上、来院してもらうなどが考えられる（この場合でも同意の記録が残るようにすることが望ましい）。

C．最低限のガイドライン

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。

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。

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。

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。

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)。

A．３．４．２．８　個人データの提供に関する措置

A．JIS Q 15001：附属書A（管理策）

組織は、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、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、及び取得方法を通知し、本人の同意を得なければならない。ただし、次に掲げる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) 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) 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、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)～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が提供された場合であって、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

B．保健医療福祉分野としての解釈

民間保険会社等の求めに応じて診断書や意見書を作成する場合、学校や職場からの病状問い合わせ、警察等からの問い合わせ、医学教育及び研修への利用、外部評価機関の評価の

ための診療情報の閲覧などであらかじめ同意を得ていない場合がこの項に相当する。行政機関による医療監視や裁判所の命令による利用、感染症予防法等による情報提供は法令に基づくためにかならずしも同意は必要としないが、公益目的による除外は慎重に判断しなければならない。当該個人情報の提供がおこなわれなければ公益を大きく損なう場合だけに限定するべきである。

患者等が意識障害、精神障害、乳幼児等で、同意を得られない場合がある。この場合、提供する情報が、保健医療福祉サービスの遂行上の必要性及び公益性が高い場合は、本人の同意なしに提供を行うことができると考えるべきである。しかし、これらの場合でも親権者、保護者が定まっている場合は、可能な限り親権者又は保護者の同意を得る必要がある（虐待の可能性がある場合を除く）。

ただし書きｆ）に該当する事例は、地域医療連携などで、医療機関間で患者情報を共有している場合や病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人データを特定の者との間で共同して利用することが予定されている場合などが該当する。共同利用者（連携元）が、ｆ）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、本人に通知し、又は本人が容易に知り得る状態に置いている場合は、共同利用者（連携先）は、第三者には該当しないことから、本人の同意は不要である。ただし、共同利用者（連携先）が、受領した個人情報を使って本人に連絡又は接触する場合は、A.3.4.2.7 のただし書きｄ）が適用されることに注意すること。

警察や検察等捜査機関からの照会や事情聴取は、A.3.4.2.3 のただし書きａ）に該当し、本人の同意を得ずに個人データを提供することができる。ただし、提供の際には、当該情報提供を求めた捜査官の役職、氏名を確認するとともに、提供内容、対応者、任意捜査か否か等の情報を記録しておくことが望ましい。

Ｃ．最低限のガイドライン

① 本措置を実施するための手順を規定すること。

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。

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）。

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。

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）。

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）

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

D．推奨されるガイドライン

法令上の定めにより個人情報を提供する場合は、A.3.4.2.3 のただし書きのａ）により本人の同意は不要であるが、保健医療福祉分野の事業者が取り扱う要配慮個人情報の提供は、注意を要するため、できるかぎり本人に説明し、同意を得ておくことが望ましい。もし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。

A．３．４．２．８．１　外国にある第三者への提供の制限

A．JIS Q 15001：附属書A（管理策）

組織は、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及びその他の法令等によって除外事項が適用される場合は、本人の同意を得ることを要しない。

B．保健医療福祉分野としての解釈

旧個人情報保護法においても、第三者への提供について規定されていたものの、第三者については国内・国外の区別はされていなかった。しかし、情報通信技術の発展に伴う個人情報の利用形態の多種多様化により、個人データが外国に提供されるケースが増加していることと、ＥＵのデータ保護指令のような、個人情報の保護に関する国際的な枠組みと整合性をとっていくという観点から、改正個人情報保護法第 24 条において、外国にある第三者への提供の制限が規定され、原則として第三者提供の同意とは別に、外国にある第三者への提供を認める旨の同意をあらかじめ得なければならないこととなった（個人情報保護法第 24 条）。

保健医療福祉分野においては、症例研究等において患者の診療情報等の個人データを扱っており、外国にある第三者との共同研究も多く行われていることから、個人データを外国

にある第三者へ提供する場合は、法律・ガイドラインに基づいた対応が必要となる。

C．最低限のガイドライン

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。

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）。

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）。

A．３．４．２．８．２　第三者提供に係る記録の作成など

A．JIS Q 15001：附属書A（管理策）

組織は、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、保管しなければならない。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、又は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) 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置いているとき

B．保健医療福祉分野としての解釈

改正個人情報保護法では、個人データの第三者提供に関しては、“本人同意を得ている旨”及び“いつ、誰が、誰に、どの様な個人情報を提供したか”の記録を作成、保管することが義務付けられており、また、個人情報を第三者から取得した場合においても、同様の措置を講じることが義務付けられている。この法的な措置は、複数の名簿業者を介して個人情報が転売されることによる不正な情報拡散を防止するために、第三者提供に関わる事業者にトレーサビリティの確保を義務付けることを目的としている。保健医療福祉分野においては、「個人情報保護法」第 25 条、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」Ⅲ．7 (1)④でも、医療介護等に必要である紹介状等を紹介先医療機関へ提供するなどの第三者提供については本人に代わって個人データを提供していると見做され、トレーサビリティは義務付けられていない。さらに、家族等への病状説明についても、本人と一体であると評価できる関係にある者に提供する場合は、本人側に対する提供と見做さ

れ、トレーサビリティは義務付けられない。

ただし、医療連携を含む直接的な診療ではない、医学研究のような２次利用に係る第三者提供では、提供に関する記録の作成と受領の際の記録の確認が求められており、以下に示す一部の事例を除いては厳格に遵守することが求められる。

１）他の病院、診療所、助産所、薬局、訪問看護ステーション、介護サービス事業者等との連携

２）他の医療機関等からの照会への回答

３）患者の診療等に当たり、外部の医師等の意見・助言を求める場合

４）審査支払機関又は保険者からの照会への回答

５）医師賠償責任保険などに係る医療に関する専門の団体、保険会社等への相談又は届出等

６）検体検査の委託、保険事務の委託、事業者等からの委託を受けて実施した健診結果の事業者への結果の通知等

７）家族等への病状説明

なお、トレーサビリティが義務付けられていない第三者提供であっても、本認定指針においては A.3.4.3.2 安全管理措置の観点から、医療機関等の部門においては、少なくとも“いつ”、“誰が”、“何（誰のもの）を”、“どこに送付したか”等の記録を残す必要がある。(A.3.4.3.2 Ⅰ.組織的安全管理措置 2))

C．最低限のガイドライン

① 医療連携を含む直接的な診療以外の目的で個人データを第三者に提供した場合、記録を作成、保管していること。

② 記録には以下の様な事項を記載すること。

- ○ 本人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

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)。

A．３．４．２．８．３　第三者提供を受ける際の確認など

A．JIS Q 15001：附属書A（管理策）

組織は、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わなければならない。ただし、A.3.4.2.3 の a)～d)のいずれかに該当する場合、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。 組織は、法令等の定めるところよって確認の記録を作成、保管しなければならない。

B．保健医療福祉分野としての解釈

A.3.4.2.8.2 で示している通り、個人データの受領者においても、「個人情報保護法」第26 条、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」Ⅲ.8(1)では保健医療福祉サービスの提供に必要である個人データの受領については確認・記録作成義務は適用されないとしているが、２次利用に係る第三者提供では、提供に関する記録の作成と受領の際の記録の確認が求められることとなる。

なお、記録とは、書面又は電子データ、もしくは記録すべき事項がログ、IP アドレスなどの一定の情報を分析することによって明らかになることをいう。

C．最低限のガイドライン

① 医療連携を含む直接的な診療以外の目的で第三者から個人データの提供を受けるに際しては、確認を行った記録を作成し、保管していること。

② 確認を行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

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。

A．３．４．２．９　匿名加工情報

A．JIS Q 15001：附属書A（管理策）

組織は、匿名加工情報の取扱いを行うか否かの方針を定めなければならない。 組織は、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適切な取扱いを行う手順を確立し、かつ、維持しなければならない。

B．保健医療福祉分野としての解釈

改正個人情報保護法では、新たに「匿名加工情報」という概念が新設された。「匿名加工情報」とは、個人情報を個人情報の区分に応じて定められた措置を講じて特定の個人を識別することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものをいう。また、個人情報から匿名加工情報を作成する場合には、個人情報保護委員会規則で定める基準に従って加工する等一定の制限を受けることとなり、その基準に従って、適切な加工を行う必要がある。匿名加工情報の加工基準としては、主に次のような5点を挙げている。

(1) 特定の個人を識別することができる記述等の削除
(2) 個人識別符号の削除
(3) 情報を相互に連結する符号の削除
(4) 特異な記述等の削除
(5) 個人情報データベース等の性質を踏まえたその他の措置

(1) は、氏名、性別、住所、生年月日など特定の個人を識別できる記述等を全部またはその一部を削除する、あるいは他の記述などに置き換えることによって、特定の個人を識別できないようにすることである。例）氏名、住所、生年月日を削除、又は住所は○○県△△市、生年月日は生年月に置き換えるなど

(2) の個人識別符号の削除とは、個人の身体の一部の特徴をコンピュータなどで利用する際に変換した符号（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋などの生体情報）のうち、特定の個人を識別するに足りるものとして規則で定める基準に適合するものである。また、旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証の番号などの公的機関が割り振る番号なども該当する。

(3) の情報を相互に連結する符号とは、例えばサービス会員の情報について、氏名などの基本的な情報と購買履歴を分散管理し、それらを連結するために付された管理用 ID などのことであるが、これらの符号についても、削除するか、連結にかかわらない他の符号に置き換えなければならない。

(4) の特異な記述とは、珍しい事実に関する記述等や他の個人と著しい差異が認められる記述等で、例えば症例数の極めて少ない病歴、あるいは年齢が「116歳」といった記述などを指す。極めて少ない病歴などは削除、116歳という情報は「90歳以上」といった記述に置き換えなければならない。

(5) 個人情報データベース等の性質を踏まえたその他の措置とは、(1)～(4)の加工を施した情報であっても、個人情報データベース等の性質により、特定の個人を識別することが可能である状態、あるいは元の個人情報を復元できる状態のままである場合にはさらに加工する必要があるということで、想定される事例としては、自宅や職場などの所在が推定できる位置情報、小売店での購入者が極めて限定されている商品の購買履歴、小学校の身体検査で１人の児童の情報が他の児童とは異なる場合などが挙げられる。

改正個人情報保護法において、この「匿名加工情報」の定義が明確にされたことで、個人情報保護委員会が定めた匿名加工情報の作成に関する基準に従って、適切な加工を行った「匿名加工情報」については、本来の利用目的外での利用が可能になり、第三者提供においても、第三者提供時に公表等を行うことで本人の同意なく提供が可能となった。

保健医療福祉分野においては、「医療分野の研究開発に資するための匿名加工医療情報に関する法律」（次世代医療基盤法）が平成29年5月に公布され、平成30年5月の施行が予定されている。同法は、医療分野の研究開発を促進するために、特定の個人が識別できな

いようにした匿名加工情報を活用していくための法律である。保健医療福祉分野における匿名加工情報の取り扱いについては、症例数の極めて少ない病歴（処方内容も含む）は、特定の個人の識別又は元の個人情報につながるおそれがあるということと、個人識別の可能な医療情報は、その漏えいによって不名誉、不利益、場合によっては差別まで生む可能性があることから、症例数の極めて少ない病歴（処方内容も含む）のような特異な記述等については、削除又は他の記述等への置き換えを行なわなければならない。また、データの利活用という観点から特異な記述等の削除又は他の記述等への置き換えを行なわない場合は、要配慮個人情報に該当する。

従って、特異な記述等の削除又は他の記述等への置き換えを行なわない情報の取得および利用、提供については、A.3.4.2.3 C① に準じた措置が必要である。

以下に示すC．最低限のガイドラインは、個人情報保護委員会規則で定める基準に従って加工された匿名加工情報を取り扱う場合の管理策である。

C．最低限のガイドライン

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。
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。
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。
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。
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）。
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。

A．３．４．３　適正管理

A．３．４．３．１　正確性の確保

A．JIS Q 15001：附属書A（管理策）

組織は、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、最新の状態で管理しなければならない。 組織は、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するよう努めなければならない。

B．保健医療福祉分野としての解釈

本管理策は、個人情報に関して誤った情報や古い情報によって個人の利益が侵害されることを防ぐため、利用目的に応じて必要な範囲において、正確かつ最新の状態で個人情報

を管理することを求めるものである。特定された個人情報に関し正確性に対するリスクを認識し、その対策をルール化することが求められる。データの誤りは、誤った指示、誤処理、誤操作、機器等の故障等によっても発生するので、その原因を除去することにより防止しなければならない。次に正確性の確保に関する留意ポイントを示す。

（1）入力時のチェック

情報システムへの入力時、確定操作前に入力データに誤りがないか、転記ミスがないかを十分チェックする習慣及びチェックできるシステムにする必要がある。

（2）変更の時間的ズレによる正確性の喪失

記録の遅れ、あるいは住所・姓名等の変更が迅速に反映されないため、正確性が喪失される場合がある。住所変更、保険証区分等の変更や診療録等の記載の訂正に対して誰が変更を行えるのか、またその変更や訂正に対する履歴はどのように管理するのかをルール化する必要がある。

（3）システムによる正確性確保とその検証

情報システムは指示書に基づく処理、データのタイムスタンプ、件数チェック、運用の自動化等により正確性が確保される。また処理結果の確認、実施記録の保管、指示書とオペレーションログの検証等が行われ正確性が検証される。

（4）個人データの消去について

改正個人情報保護法第 19 条において、個人データ消去の努力義務について新設された。正確かつ最新の状態で個人情報を管理しているか、事業者が定めた保管期限を過ぎた個人情報について、消去・廃棄が行われていることと、その記録を残す必要がある。

（4）情報システムの技術的対策

- 用語・コードのマスターの種別あるいはバージョン管理を適正に行うこと
- 患者名等により各データの所在管理が確実におこなわれる仕組みをもつこと
- 住所や保険区分等の変更があった場合に変更が可能でなお変更履歴が残ること
- 入力の確定操作後は変更が出来ない機構であること

（5）管理規程の整備

- 運用管理（データ利用、ジョブ処理、ファイル取扱、機器操作等）
- 入出力管理（入力処理、出力処理、本人確認方法、記録事項変更確認方法、誤データ更新方法等）
- データ管理（データ保管、バックアップ、保管期限・廃棄等）
- 委託先管理（自施設と同じ管理レベルの正確性の確保を委託先に要求する）

C．最低限のガイドライン

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）。

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）
- 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）。

D．推奨されるガイドライン

① 論理的にありえない入力を行った時は、警告を発生する機能をシステムとして付加することが望ましい。特に正確性を要するデータやインデックスは２重化が望ましい。

② 確実に本人が署名を行ったことを確認することが必要な場合は、電子署名の手段によりデータの正確性をデジタル的に確認できるシステムの導入を推奨する。

③ データの前後関係を明らかにすることが必要なデータに対しては、証拠性のあるシステムによるタイムスタンプを付ける等の時刻管理を行うことが望ましい。

④ 個人情報の内容の正確性、最新性を確保するため、委員会等において、具体的なルールを策定したり、技術水準向上のための研修の開催などを行うことが望ましい。

⑤ アクセスログ等の情報システムに関する記録の正確性を確保するため、時刻情報は標準時刻と一致させておく仕組みを導入することが望ましい。

A．３．４．３．２　安全管理措置

A．JIS Q 15001：附属書A（管理策）

組織は、その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個人情報の安全管理のために必要かつ適切な措置を講じなければならない。 安全管理措置に関する管理目的及び管理策は、附属書Ｃを参照。

B．保健医療福祉分野としての解釈

（１）安全管理のために必要かつ適切な措置

「適切な措置」という意味は、脅威が発生した場合の損失や平常時の対策状況に対する社会的評価を配慮して、経済的に実行可能な最良の技術及び運用方法の適用に配慮することである。その為にはA.3.3.3で認識したリスク及びその対策を技術的に配慮した管理規程の作成、及びそれに基づいた運用が必要である。

また、漏えい、滅失、き損の防止、その他の個人情報の安全管理のため、組織的、人的、物理的及び技術的安全管理措置を講じなければならない。その際、本人の個人情報が漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人情報の取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。なお、その際には、個人情報を記録した媒体の性質に応じた安全管理措置を講ずること。特に、施設全体及び個人情報取扱場所への入退に関する情報を記録し確認することは物理的安全管理のための基本である。少なくとも最初に開錠した時刻・人、最後に施錠した時刻・人を記録する手段を確立すること。

（２）内部の脅威に対する抑制

一般的に、個人情報の漏えい事例は内部のものによって行われることが多いので、医療施設でもその脅威に対する対策が必要である。特に内部のものが安全性を脅かす誘惑にかられないようにするためにも、アクセスログを取っていることや個人認証を行っていることを周知させるような明確な規制が有効である。

（３）一覧機能、検索機能、コピー機能の制限

特に患者等のデータを一覧表として表示できる機能、患者名等から診療データを検索できる機能のアクセス制限や表示データの外部記憶媒体へのコピー制限機能等が重要である。また、アクセス可能者が、患者等からの同意の得られた範囲で運用できるための機能が必要となる。

（４）紙データや検体の授受を含めた管理

コンピュータ内のデータのみでなく、記入用紙あるいは出力用プリント・オーダ伝票あるいは診療録等の紙データの閲覧及び移動時の取扱いも管理規程を定め、入退出者を監視したり、第三者に覗き見されるような不用意な場所への放置や、搬送時の安全対策により紛失や第三者への漏えいを防止しなければならない。

また、臨床検査等を外部へ依頼する際も、検体等やレポートの授受に関する安全対策について委託業者も含めた形で管理規程を定めておく必要がある。

（５）個人用コンピュータの管理

医師等が自己の研究用又は診療の必要から、パーソナルコンピュータに個人情報をデータベース化している場合も禁止するか、適正運用管理の為のルール化を行っておく必要がある。個人情報（診療情報等）の持ち出しについては、原則として禁止することが望ましい。

（６）廃棄時の安全性

個人情報の漏えい事例には、破棄時の漏えいが多くみられることから、廃棄にあたっても、電子ファイルの場合は二重書き消去、あるいは、個人情報が打ち出された紙の場合は破砕処理あるいは溶解処理などによって、破棄されたデータが他者に流出することのないよう留意することが必要である。個人情報を取り扱った情報機器を廃棄する場合についても、記憶装置内の個人情報を復元不可能な形に消去して廃棄すること。特に、処方箋の廃棄について

は、管理者の承認の下に行うことが法令で求められていることから、具体的な廃棄の記録を残すことは重要である。

また、医療機関等で発生する点滴ボトル（ラベルに個人情報の記載有り）等の廃棄に際しても、個人情報が判読できないように確実に破砕されることを確認すること。廃棄業務を委託する場合には、これらのことを委託契約において明確に定めること。

（７）プライバシーへの配慮

受付での呼び出しや、病室・居室における患者等の名札の掲示などについては、取り違え防止など業務を適切に実施する上で必要と考えられるが、プライバシー保護の重要性にかんがみ、患者等の希望に応じて一定の配慮をすることが望ましい。

（８）SNS を利用して医療情報連携等を行う場合の考え方

クラウドサービスと同様に、SNS（Social Network Service）の普及により、医療情報連携等において SNS を利用するケースが増えてきている。また、SNS を利用した医療情報連携は、自治体や医師会主導で行われることが多くなっており、SNS で共有する情報についても、患者のプライバシーに係るセンシティブな情報が含まれるため、利用する SNS について正しい知識を持ち、リスクを認識したうえで利用する必要がある。このため、本認定指針においても A.3.4.3.2.C⑥で SNS 利用時の管理策を示すことにした。

なお、SNS を利用する際に気を付けるべき事項として、一般社団法人　保健医療福祉情報安全管理適合性評価協会（HISPRO)のホームページにおいて具体的な対策が示されているので参考されたい。

URL：http://www.hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf#toolbar=0

Ｃ．最低限のガイドライン

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)。

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。

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)。

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。

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

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。

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。

D．推奨されるガイドライン

①　不正ソフトウェアを自動的に監視し、活性化しない機構を備えることが望ましい。

②　秘密鍵等のシステム内での保管は、ハードウエアセキュアモジュールなどへの格納が望ましい。

③　情報システムの認証に用いられる手段として、2 要素認証を実施している、もしくは、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上の認証がなされていることが望ましい。

A．3．4．3．3　従業者の監督

A．JIS Q 15001：附属書A（管理策）

組織は、その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わなければならない。

B．保健医療福祉分野としての解釈

医療機関等は、A.3.4.3.2 の安全管理措置が図られるよう、従業者に対し必要かつ適切な監督を行わなければならない。なお、「従業者」とは、医療資格者のみならず、当該医療機関等の指揮命令を受けて業務に従事する者すべてを含むものであり、また、雇用関係のある者のみならず、理事、派遣労働者、ボランティア等も含むものである。

医療法第 15 条では、医療機関の管理者には、勤務する医師等の従業者の監督義務が課せられていることを認識すべきである。薬局や介護関係事業者についても、薬事法や介護保険法に基づく「指定居宅サービス等の事業の人員、設備及び運営に関する基準」、「指定居宅介護支援等の事業の人員及び運営に関する基準」、「指定介護老人福祉施設の人員、設備及び運営に関する基準」、「介護老人保健施設の人員、施設及び設備並びに運営に関する基準」及び「指定介護療養型医療施設の人員、設備及び運営に関する基準」等に同様の規定がある。

C．最低限のガイドライン

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。

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。

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。

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。

A．3．4．3．4　委託先の監督

A．JIS Q 15001：附属書A（管理策）

組織は、個人データの取扱いの全部又は一部を委託する場合は、特定した利用目的の範囲内で委託契約を締結しなければならない。

組織は、個人データの取扱いの全部又は一部を委託する場合は、十分な個人データの保護水準を満たしている者を選定しなければならない。このため、組織は、委託を受ける者を選定する基準を確立しなければなければならない。委託を受ける者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ことを含めなければならない。

組織は、個人データの取扱いの全部又は一部を委託する場合は、委託する個人データ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督を行わなければならない。

組織は、次に示す事項を契約によって規定し、十分な個人データの保護水準を担保しなければならない。

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、又は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

組織は、当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならない。

B．保健医療福祉分野としての解釈

医療機関等が、検査や保険請求業務の外注を行うことは一般的となってきており、外注に際して個人データをどのように保護するかは重要な事項である。

検査や診療報酬又は介護報酬の請求に係る事務等、個人データの取扱いの全部又は一部を委託する場合、A.3.4.3.2 に基づく安全管理措置を遵守させるように受託者に対し必要かつ適切な監督をしなければならない。「必要かつ適切な監督」には、委託契約において委託者である医療機関等が定める安全管理措置の内容を契約に盛り込み、受託者の義務とすること。および業務が適切に行われていることを、定期的に確認することなども含まれる。

委託先の監督の前提として、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然に求められることである。必要のない個人データを提供した結果、委託先が個人データを漏えいした場合には、必要かつ適切な安全管理措置を講じていたとはみなされないことにも留意すべきである。

（１）委託先評価基準

個人情報保護に関する評価基準を明確にする必要がある。もちろん、プライバシーマークを取得している業者が好ましいといえるだろう。しかし、プライバシーマークを取得していない業者であっても、個人データの保護に努めている事業者もあるので、次のような具体的かつ客観的な評価基準で個人データを適切に取り扱っている事業者を委託先（受託者）として選定すること。

○　個人情報保護方針を制定している。
○　個人情報保護に関する責任者及び情報システム管理者を選任している。
○　委託された個人データの取り扱い手順、安全管理方法が明文化されている。
○　委託先の安全管理措置が、A.3.4.3.2 の最低限のガイドラインと同等である。
○　就業規則等で守秘義務を定めている。
○　退職後も守秘義務を課している。
○　個人情報保護に関する研修教育を定期的に行っている。
○　情報システムのセキュリティ仕様を明示でき、その内容が十分である。

（２）委託先との契約書

委託先選定基準による評価の上、合格した事業者と委託契約を取り交わすことになる。契約内容は、ａ）～ｈ）及び以下の点に留意すること。

○　契約において、個人データの適切な取扱いに関する内容を加える（委託期間中のほか、委託終了後の個人データの取扱いも含む）。
○　受託者が、委託を受けた業務の一部を再委託することを予定している場合は、再委託を受ける事業者の選定において、個人データを適切に取り扱っている事業者が選定されるとともに、再委託先事業者が個人データを適切に取り扱っていることが確認できるよう契約において配慮する。
○　受託者が個人データを適切に取り扱っていることを定期的（少なくとも年１回）に確認する。
○　受託者における個人データの取扱いに疑義が生じた場合（患者等からの申出があり、確認の必要があると考えられる場合を含む。）には、受託者に対し説明を求め、

必要に応じ改善を求める等、適切な措置をとる。

○　委託する業務に応じ、関連する以下の通知等を遵守すること。

- 「医療法の一部を改正する法律の一部の施行について」（平成 5 年 2 月 15 日健政発第 98 号）の「第 3　業務委託に関する事項」
- 「病院、診療所等の業務委託について」（平成 5 年 2 月 15 日指第 14 号）

○　個人データの取り扱いの外部委託（病理検査や遠隔画像診断等）に際して、後日の確認のため結果報告後も個人データ（組織標本や画像データ等）を長期間委託先に保管する場合は、その旨を委託契約書等に明記するとともに、保管期限も規定する必要がある。本人の知らない場所に、個人データが長期間保管されることは、第三者提供及び個人情報の自己コントロール権の侵害に当たるとも考えられる。少なくとも、個人データを委託先で保管すること、及び保管期限（廃棄手順を含む）について契約書等で明確にする必要がある。

（8）クラウドサービスを利用する際の考え方

近年、医療業界においても電子カルテ等の医療情報システムのクラウド化が期待され、実際にクラウドを利用したサービスも普及拡大してきているが、医療情報は患者のプライバシーに係るセンシティブな情報が含まれていることから、漏洩等の事故が発生すると患者および医療機関に多大な被害が及ぶこととなる。そのため、保健医療福祉分野においてクラウドサービスを利用して患者等の個人データを利用する場合は、クラウドサービス事業者へ外部委託をする際に医療機関等が追うべき責任、委託契約を締結する際に確認すべきことなど、クラウドサービスが抱えるリスクを認識したうえで利用する必要がある。

特に、取り扱う情報として、法令により作成や保存が定められている文書を含む場合には、「医療情報システムの安全管理に関するガイドライン」において、「医療情報を受託管理する情報処理事業者向けガイドライン」及び「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」に準拠することが定められており、医療情報システム及び医療情報が国内法の適用が及ぶ範囲にあることを確実とすることが必要である。

C．最低限のガイドライン

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。

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。

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。

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。

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。

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）。

⑦ 委託先と、特定した利用目的の範囲内で委託契約を締結していること。

⑧ 契約終了後も、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。

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）。

⑩ 委託契約書が当該個人データの保有期間にわたって保存されていること。

⑪ 委託契約に基づき、委託先を適切に監督していること。

⑫ クラウドサービスを利用して医療情報等の利用・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）。

D．推奨されるガイドライン

① 基本的にプライバシーマーク取得者に対して委託を行うようにすることが望ましい。

② 人材派遣事業者との人材派遣契約、清掃事業者や廃棄事業者との契約、オフィスの賃貸借契約等は、個人データの取扱いを含まない限り、本管理策の対象外である。これらは安全管理措置（A.3.4.3.2）に含まれるものであり、このような事業者とは守秘義務に

関する事項を盛込んだ契約を締結することが望ましい。

③ 国が定めた資格が必要で、かつ法律により守秘義務を課されている者（弁護士、社会保険労務士、公認会計士、医師等）は、それだけで選定基準を満たしていると評価でき、選定基準による選定は必須ではないが、守秘義務に関する事項を盛込んだ契約を締結することが望ましい。

④ 契約には、契約先で個人がデータを取り扱う者の役職又は氏名等に関する事項を明記することが望ましい。

⑤ 定期的に（少なくとも年１回）委託業務の監査を実施すること等により、委託内容の実施状況等を評価することが望ましい。

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

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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なければならない。ただし、次に掲げるいずれかに該当する場合は、保有個人データには当たらない。

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する、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及び秩序維持に支障が及ぶおそれのあるもの

組織は、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様に取り扱わなければならない。

Ｂ．保健医療福祉分野としての解釈

保健医療福祉分野で取り扱うカルテ等の諸記録には、検査結果のような客観的なデータもあれば、それに対して医師等が行った主観的な判断や評価も書かれている。これら全体が患者等個人に関する情報に当たるものであるが、あわせて、当該診療録を作成した医師等の側からみると、自分が行った判断や評価を書いているものであるので、医師等個人に関する情報とも言うことができる。従って、診療録等に記載されている情報の中には、患者等と医師等双方の個人情報という二面性を持っている部分もあることに留意が必要である。ただ

し、診療録等の全体が患者等の保有個人データであることから、本人から開示の求めがある場合に、その二面性があることを理由に全部又は一部を開示しないことはできない。

ただし書きａ）～ｄ）に該当する事例は次の通りである。医療機関等ではａ）及びｄ）などが該当すると考えられる。特に、要人等の診療情報の有無などもただし書きに該当し、保有個人データではない。

ａ）の場合とは、例えば、児童虐待の被害者の支援団体が、家庭内暴力の加害者（配偶者又は親権者）及び被害者（配偶者又は子）を本人とする個人情報を持っている場合などをいう。

ｂ）の場合とは、例えば、いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人情報を持っている場合や、不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人情報を保有している場合などをいう。

ｃ）の場合とは、例えば、製造業者、情報サービス事業者等が、防衛に関する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人情報を保有している場合や、要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合などをいう。

ｄ）の場合とは、例えば、警察からの捜査関係事項照会や捜査差押令状の対象となった事業者が、その対応の過程で捜査対象者又は被疑者を本人とする個人情報を保有している場合などをいう。

Ｃ．最低限のガイドライン

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。

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）。

Ｄ．推奨されるガイドライン

① ただし書きに該当する可能性のある個人情報についての開示の可否については、医療機関等の内部に設置する倫理委員会等において検討した上で速やかに決定することが望ましい。

Ａ．３．４．４．２　開示等の請求等に応じる手続

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、開示等の請求等に応じる手続として次の事項を定めなければならない。 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

組織は、本人からの開示等の請求等に応じる手続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しなければならない。

組織は、A.3.4.4.4 又はA.3.4.4.5 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、その額を定めなければならない。

Ｂ．保健医療福祉分野としての解釈

開示等に関して、受付窓口、請求のための様式、開示等の求めに応じる範囲（代理人等）、手数料の額等の具体的手続きを定める必要がある。判断項目・判断基準、対応スケジュール、本人確認の方法等についても定め、開示申し込み窓口には適切な対応が出来る従業者を配置すること。窓口は専用でなく、その他の相談業務の窓口と兼ねても良い。手数料の額は抑止的であってはならず、それに応じる上で必要な通信費などの実費を勘案して合理的であると認められる範囲内でその額を定めなければならない。

開示等については、本人のほか、①未成年者又は成年被後見人の法定代理人、②開示等の求めをすることにつき本人が委任した代理人により行うことができる。

開示の求めを行い得る者から開示の求めがあった場合（代理人等）、原則として本人に対し保有個人データの開示を行う旨の説明を行った後、開示の求めを行った者に対して開示を行うものとする。代理人等からの求めがあった場合で、①本人による具体的意思を把握できない包括的な委任に基づく請求、②開示等の請求が行われる相当以前に行われた委任に基づく請求が行われた場合には、本人への説明に際し、開示の求めを行った者、及び開示する保有個人データの内容について十分説明する必要がある。

手数料を徴収できるのは、“A.3.4.4.4 保有個人データの利用目的の通知”及び“A.3.4.4.5 保有個人データの開示”に係る場合のみである。

当該本人の保有個人データが多岐にわたり、データ量が膨大であるなど、全体の開示等が困難又は非効率な場合は、本人の意思を尊重しつつ、本人に過去の受診の状況、病態の変化等の概要を説明するなど、本人が開示等の求めを行う情報の範囲を特定できるよう配慮すること。

開示手続きは、以下の点に留意しつつ保有個人データの開示の手続を定めること。

- 請求のための様式、代理人等開示の求めに応じる範囲、応じない場合の判断基準・承認手順、対応スケジュール等の具体的手続き、本人（又はその代理人）確認の方法等
- 開示等の求めの方法は書面によることが望ましいが、患者等の自由な求めを阻害しないため、開示等を求める理由を要求することは不適切
- 開示等の求めがあった場合、主治医等の担当スタッフの意見を聴いた上で、速やか

に保有個人データの開示等をするか否か等を決定し、これを開示の求めを行った者に通知する

- 保有個人データの開示を行う場合には、日常の保健医療福祉サービス提供への影響等も考慮し、本人に過重な負担を課すものとならない範囲で、日時、場所、方法等を指定することができる

C．最低限のガイドライン

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）。

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

－開示等の求めをすることにつき本人が委任した代理人

－患者が成人で判断能力に疑義がある場合は、現実に患者の世話をしている親族、及びこれに準ずる者（診療情報の開示）

③ 従業者への対応手続きも規定すること。

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。

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。

D．推奨されるガイドライン

開示の判断・スケジュール等は標準的なものを明示することが望ましい。

A．３．４．４．３　保有個人データに関する事項の周知など

A．JIS Q 15001：附属書A（管理策）

組織は、当該保有個人データに関し、次の事項を本人が知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む。）に置かなければならない。

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

B．保健医療福祉分野としての解釈

保有個人データについて、その利用目的、開示、訂正、利用停止等の手続の方法、及び利

用目的の通知又は開示に係る手数料の額、苦情の申出先等について、少なくとも院内や事業所内等への掲示、あるいは患者等からの要望により書面を交付、問い合わせがあった場合に具体的内容について回答できる体制等を確保する必要がある。

本管理策の C)で求めている利用目的は、保有個人データの利用目的であり、開示対象ではない委託された個人データの利用目的等は含まれない。従って、本管理策の利用目的と A.3.4.2.4 で求める利用目的とは異なることを理解すること。

→付録24　医療機関における保有個人データの周知に関する文書の例

C．最低限のガイドライン

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。

A．３．４．４．４　保有個人データの利用目的の通知

A．JIS Q 15001：附属書A（管理策）

組織は、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なければならない。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、理由を説明しなければならない。

B．保健医療福祉分野としての解釈

本管理策は、保有個人データに関する周知事項として、医療機関等が A.3.4.4.3 のｃ）に基づいて公表している利用目的について、本人から利用目的の通知を求められた場合に応じること、及び応じない場合について定めたものである。本人が、公表されている利用目的だけでは医療機関等が取り扱う保有個人データの利用目的を十分に把握できない場合に該当する。利用目的を個別にできるかぎり詳細に特定し（“・・・の治療のため・・・に利用する”など）本人に通知することが望まれる。利用目的の特定・通知に際して手数料がかかる場合は、その手数に対して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、その額を定めることが出来る。

本人から求められた保有個人データの利用目的の通知、開示、訂正等、利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨本人に通知する場合は、本人に対して、その理由を説明するよう努めなければならない。本人に対して理由を説明する際には、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが望ましい。

C．最低限のガイドライン

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。

② 本人から当該本人が識別される保有個人データについて、利用目的の通知を求められた場合、遅滞なくこれに応じていること。

③ 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）。

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。

A．３．４．４．５　保有個人データの開示

A．JIS Q 15001：附属書A（管理策）

組織は、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き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（開示の請求などを行った者が同意した方法があるときは、当該方法）によって開示しなければならない。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、理由を説明しなければならない。

a）本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

b）当該組織の業務の適正な実施に著しい支障を及ぼすおそれがある場合

c）法令に違反する場合

B．保健医療福祉分野としての解釈

本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、書面の交付による方法等により、遅滞なく、当該個人情報を開示しなければならない。しかし、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しないことができる。個々の事例への適用については個別具体的に慎重に判断することが必要である。

a）の場合とは、患者等の本人の状況等について、家族や本人の関係者が医療機関等に情報提供を行っている場合に、これらの者の同意を得ずに本人自身に当該情報を提供することにより、本人と家族や関係者との人間関係が悪化するなど、これらの者の利益を害する恐れがある場合や、症状や予後、治療経過等について本人に対して十分な説明をしたとしても、本人に重大な心理的影響を与え、その後の治療効果等に悪影響を及ぼす場合などをいう。

b）の場合とは、同一の本人から複雑な対応を要する同一内容について繰り返し開示の求

めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ちゆかなくなる等、業務上著しい支障を及ぼす恐れがある場合などをいう。

開示の方法は、書面の交付又は求めを行った者が同意した方法によること。また、求められた保有個人データの全部又は一部について開示しない旨を決定したときは、本人に対し、遅滞なく、その旨を通知しなければならない。また、本人に通知する場合には、本人に対してその理由を説明するよう努めなければならない。

法令の規定により、保有個人データの開示について定めがある場合には、当該法令の規定によるものとする。ただし書きａ）～ｃ）に該当するため、開示できない旨を本人に対して理由を説明する際には、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが望ましい。

Ｃ．最低限のガイドライン

① 開示のための具体的手順（様式等）を規定すること。

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）。

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。

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。

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。

Ｄ．推奨されるガイドライン

① 開示の対象となる保有個人データは、自己を本人とする個人情報である。従って、本人以外の者が識別される保有個人データは、本管理策に基づいて開示の求めがなされても、その対象には含まれない。その場合の開示に際しては本人以外の個人情報を削除するか判別できない状態にすることが望ましい。

② 委託を受けて取り扱っている個人情報は、保有個人データには当たらない。しかし、本人から開示の求めがあった時は、その旨を説明すると共に、当該個人情報の開示の権限を有する委託元を明らかにするなどの対応を行うことが望ましい。

Ａ．３．４．４．６　保有個人データの訂正、追加又は削除

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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わなければならない。また、組織は、訂正等を行わない旨の決定をしたときは、その旨及び理由を、本人に対し、遅滞なく通知しなければならない。

B．保健医療福祉分野としての解釈

訂正又は削除を行うのは、当該情報が誤っていることが判明した場合に限ることが必要である。要求されたからといって客観的な事実で診療上必要な事項は変更や削除はできない。所見などについては、明確な誤りでない限り訂正はできない。なお、「削除」と、A.3.4.4.7の「消去」とは一般に区別無く用いられることが多いが、「消去」とは、保有個人データを消してその効力を失わせることで（使えなくなる）、個人情報の内容が事実でない部分を削除して利用を続ける「削除」とは異なる。

訂正等、利用停止等又は第三者への提供の停止が求められた保有個人データの全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが必要である。

保有個人データの訂正等にあたっては、訂正した者、内容、日時等が分かるように行われなければならない。当然ながら字句などを不当に変える改ざんは、行ってはならない。

C．最低限のガイドライン

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。

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。

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。

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。

A．３．４．４．７　保有個人データの利用又は提供の拒否権

A．JIS Q 15001：附属書A（管理策）

組織が、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、これに応じなければならない。また、措置を講じた後は、遅滞なくその旨を本人に通知しなければならない。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、理由を説明しなければならない。

B．保健医療福祉分野としての解釈

本人から保有個人データの利用停止等を求められた場合は、原則として応じることを定めている。つまり、個人情報保護法（第 30 条）と異なり、保有個人データの取り扱いに手続き違反がない場合であっても、本人から利用停止等の求めがなされたときには、原則として応じることが求められている。本管理策は、保有個人データが適切に取り扱われていても、保有個人データの存在自体を消去したいという場合にも応じるという、プライバシー保護に重点を置いた規定と言える。

しかし、保健医療福祉分野の個人情報は、法令で保存期間が定められているものも多く存在するので、利用停止等の求めがあっても法令上の義務を優先する必要がある。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が求められる。

利用又は提供の拒否を求められた保有個人データの全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明すること。

C．最低限のガイドライン

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。

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。

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。

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）。

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。

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。

A．３．４．５　認識

A．JIS Q 15001：附属書A（管理策）

組織は、従業者が、7.3に規定する認識をもつために、関連する各部門及び階層における次の事項を理解させる手順を確立し、かつ、維持しなければならない。

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
　組織は、認識させる手順に、全ての従業者に対する教育を少なくとも年一回、適宜に行うことを含めなければならない。

Ｂ．保健医療福祉分野としての解釈

研修の頻度や方法等を内部規程で定め、それを遵守するものとする。採用時研修と定期研修では、もちろん内容は異なるであろうし、マネジメントシステムの制定や改定に伴う運用研修も行うことが必要である。全ての従業者が受講できるように年間計画を定め、人事記録上での取扱いも明記しておく方が効果的であると考えられる。特に、全ての従業者に個人情報保護に関する理念の理解と内部規程の遵守を求めること。また、医師や看護師等の守秘義務規定が設けられている職種については、その遵守を徹底することが重要である。研修プログラムを採用時と定期に分けて、回数・時期・内容・対象者を含めて具体的に策定すると効果的である。テキストは個人情報保護マネジメントシステム文書が基本となるが、市販されているものを利用することも可能である。

派遣労働者についても、「派遣先が講ずべき措置に関する指針」（平成 11 年労働省告示第 138 号）において、「必要に応じた教育訓練に係る便宜を図るよう努めなければならない」とされていることを踏まえ、個人情報の取扱いに係る教育研修の実施に配慮する必要がある。また、窓口業務等を業務委託した場合であっても、派遣労働者と同様に、業務委託された従業者に対する教育研修の実施に配慮すること（A.3.4.3.4 に関連）。

→付録9　教育実施報告書の様式例

Ｃ．最低限のガイドライン

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。

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。

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。

Ａ．３．５　文書化した情報

Ａ．３．５．１　文書化した情報の範囲

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。

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組織が個人情報保護マネジメントシステムを実施する上で必要と判断した記録。

Ｂ．保健医療福祉分野としての解釈

個人情報保護方針と A.3.3.5 にある内部規程、及びそれを具体化した計画、記録類が、これらに当たる。印刷物として保管しておくのもよいが、記載内容の変更に備えて加除式にしておくことが望ましい。また、イントラネット上でいつでも従業者が参照可能な状態にしておくのも役立つと思われる。

情報セキュリティマネジメントシステムや品質マネジメントシステム等の他の目的で作成された文書を、個人情報保護マネジメントシステムの一部として参照し利用する際は、文書管理の対象から外れないように、それらの文書を個人情報保護マネジメントシステムの中で規定し、必要に応じ参照できるようにしておくこと。

Ｃ．最低限のガイドライン

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。

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。

Ａ．３．５．２　文書化した情報(記録を除く。)の管理

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、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、維持しなければならない。

文書化した情報（記録を除く。）の管理の手順には、次の事項が含まれなければならない。

a) 文書化した情報（記録を除く。）の発行及び改正に関すること

b) 文書化した情報（記録を除く。）の改正の内容と版数との関連付けを明確にすること

c) 必要な文書化した情報（記録を除く。）が必要なときに容易に参照できること

Ｂ．保健医療福祉分野としての解釈

庶務や総務部門あるいは各部門に文書管理責任者を定め、要件となる文書管理を行うこととする。各種の規程や実際の運用にかかわる文書（情報開示の請求書やその処理過程の記録等）も含めて適切な管理を行う必要がある。**→付録19　文書管理台帳の例**

Ｃ．最低限のガイドライン

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。

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。

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。

Ａ．３．５．３　文書化した情報のうち記録の管理

Ａ．JIS Q 15001：附属書Ａ（管理策）

組織は、個人情報保護マネジメントシステム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、維持しなければならない。

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) 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

組織は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならない。

Ｂ．保健医療福祉分野としての解釈

記録は紙媒体である必要はなく、医療機関等において運用しやすい合理的な方法で作成すると良い。医療機関等は、必要な記録を特定し、保管方法、保管期限、及び廃棄方法等についての手順を確立し、実施し、維持しなければならない。「必要な記録を特定し」とは、記録自体も個人情報である可能性があるから、とりあえず何でも記録として残すという姿

勢ではなく、その必要性を判断すべきであるという意味である。

記録は、必要な時にすぐに検証できるように維持しておかなければならない。本管理策で必要とする記録には以下のものが含まれる。**→付録20　記録管理台帳の例**

ａ）個人情報の特定に関する記録
ｂ）法令、国が定める指針その他の規範の特定・維持に関する記録
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）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

Ｃ．最低限のガイドライン

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。
②　a)～l)の事項を含む必要な記録を作成していること。

Ａ．３．６　苦情及び相談への対応

Ａ．JIS Ｑ 15001：附属書Ａ（管理策）

組織は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順を確立し、かつ、維持しなければならない。 組織は、上記の目的を達成するために必要な体制の整備を行わなければならない。

Ｂ．保健医療福祉分野としての解釈

医療機関等は、個人情報の取扱いに関する苦情及び相談の適切かつ迅速な処理に努めなければならない。また、苦情及び相談の適切かつ迅速な処理を行うに当たり、苦情及び相談の対応窓口の設置や対応の手順を定めるなど必要な体制の整備に努めなければならない。

大規模な医療機関等の場合には、総合窓口等で受け付けるように定め、小規模な医療機関等では受診受付での対応とするのが適切である。情報開示申込窓口と同じとする場合もあるが、大規模医療機関等であれば、別にする方が客観性を保てると思われる。

代表電話の受付者に対して、苦情及び相談の担当者を告知するとともに、受診受付で苦情及び相談等の申し出があれば、相談室等へ案内し内容を担当者が聞き取る必要がある。担当

者がいない場合の対応も予め策定しておく。もちろん、開示等の請求も受け付けられるようにしても良い。

C．最低限のガイドライン

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。

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。

③ 苦情及び相談への対応を実施していること。

④ 認定個人情報保護団体の対象事業者であるときは、苦情受付時に当該団体の受付先も通知すること。

D．推奨されるガイドライン

① 患者等からの苦情及び相談の対応に当たり、専用の窓口の設置や主治医等の担当スタッフ以外の従業者による相談体制を確保するなど、患者等が相談等を行いやすい環境の整備に努めること。

② 苦情対応だけでなく、患者等が疑問に感じた内容を、いつでも、気軽に問い合わせできる相談窓口機能等を確保することも必要である。

③ 患者等の相談は、医療サービス等との内容とも関連している場合が多いことから、個人情報の取扱いに関し、患者等からの相談や苦情対応等の受付を行う窓口を設置するとともに、その窓口がサービスの提供に関する相談機能とも有機的に連携した対応が行える体制とするなど、患者等の立場に立った対応を図ることが望ましい。

④ 苦情及び相談の対応に当たり、専用の窓口の設置や主治医等の担当スタッフ以外の従業者による相談体制を確保するなど、本人が相談を行いやすい環境の整備に努めること。また、当該施設における苦情及び相談の対応体制等について院内や事業所内等への掲示やホームページへの掲載等を行うことで周知を図り、地方公共団体、地域の医師会や国民健康保険団体連合会等が開設する医療や介護に関する相談窓口等についても周知することが望ましい。

A．３．７　パフォーマンス評価

A．３．７．１　運用の確認

A．JIS Q 15001：附属書A（管理策）

組織は、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ことが組織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、維持しなければならない。 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が適切に運用されているかを確認し、不適合が確認された場合は、その是正処置を行わなければならな

い。
　個人情報保護管理者は、トップマネジメントによる個人情報保護マネジメントシステムの見直しに資するため、定期的に、及び適宜にトップマネジメントにその状況を報告しなければならない。

B．保健医療福祉分野としての解釈

　個人情報の取り扱いに不備がないことを、部署毎に責任者を決めて定期的に確認する手順を定めることが必要である。

　本管理策で求められる運用の確認のポイントとしては、A.3.3.3 で実施したリスク分析の結果、実施することとした対策が、十分でない場合は残留リスクが残る。その残留リスクが顕在化しないように、その対応をリスクの重要度に応じて“A.3.7.1 運用の点検”（日次点検、月次点検）や“A.3.7.2 内部監査”を実施することにより点検項目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ことが重要である。

　また、運用の確認とは、各部門及び各階層において行われるものである。従って、一連のマネジメントシステムの実施結果を受けて行うものではなく、日常業務において気付いた点があればそれを是正及び予防していくものであるため、大げさなものである必要はない。日常において継続的に実施できることが重要であり、部署毎の責任者が定期的に見回ってマネジメントシステムの運用状況を確認することでも良い。診察時間終了後、診察室にカルテが所定の場所に返却されずに残っていないか、検査伝票が処理されずに残っていないか、施錠忘れはないか、離席時の対処が適切か（クリアデスク、クリアスクリーンなど）などを毎日確認する。

→付録15　日常点検管理簿の例

C．最低限のガイドライン

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。

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

③ 運用の確認を実施していること。

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。

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。

A．3．7．2　内部監査

A．JIS Q 15001：附属書A（管理策）

組織は、個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を少なくとも年一回、適宜に監査しなければならない。 組織は、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、維持しなければならない。 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。

B．保健医療福祉分野としての解釈

監査が効果的にその目的を達成するためには、検討・評価の結果としての助言・勧告が、公正不偏かつ客観的なものでなければならない。また、監査活動そのものについても、他からの制約を受けることなく自由に、かつ、公正不偏な態度で客観的に遂行し得る環境であることが必要である。このため監査機能は、その対象となる諸活動についていかなる是正権限や責任も負うことなく、組織的に独立し、また、精神的にも客観的である必要がある。これらの内部監査における原則は、保健医療分野の業務が、専門性が高くかつ複雑であることから特に重要である。従って、監査で明らかになった不適合への対応は、「是正処置」で実施し、監査の延長と考えてはいけない。

当然ながら、個人情報保護監査責任者が必要に応じ「是正処置」の効果を確認し助言することを妨げるものではない（フォローアップ監査）。その際においても、個人情報保護監査責任者の責務は、効果の評価と支援であり、被監査部門及びトップマネジメントが決定した是正処置に対して承認や追加変更の指示は出来ないことを認識すべきである。

C．最低限のガイドライン

① 監査の計画及び実施、結果並びにこれに伴う記録の保持に関する責任及び権限を定める手順が規定されている。

② 個人情報保護監査責任者は、必要に応じ適切な監査員を選任し、監査計画書に従い、個人情報を取り扱う全部門に対し定期的（最低年１回）に監査を行うこと。

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）。

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。
→付録13　監査報告書の様式例

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。

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。

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。

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。

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。

→付録12　内部監査チェックリストの様式例

→付録25　JIS Q 15001:2017 準拠性監査チェックリスト例

A．３．７．３　マネジメントレビュー

A．JIS Q 15001：附属書A（管理策）

トップマネジメントは、9.3に規定するマネジメントレビューを実施するために、少なくとも年一回、適宜に個人情報保護マネジメントシステムを見直さなければならない。 マネジメントレビューにおいては、次の事項を考慮しなければならない。 a）監査及び個人情報保護マネジメントシステム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）前回までの見直しの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、国の定める指針及び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

B．保健医療福祉分野としての解釈

監査は組織の現状のルールを前提に、それが守られているかを点検するものであり、それに基づく是正も現状の枠内に止まるものである。マネジメントレビュー（A.3.7.3）は、それに止まらず、外部環境も考慮した上で、現状そのものを根本的に見直すことがあり得る点で、監査による是正とは本質的に異なることを理解すべきである。従って、監査報告に基づく是正のみでは JIS の要求を満たしているとは言えない。

C．最低限のガイドライン

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。

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。

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。

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）。

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。**→付録16　マネジメントレビュー記録の様式例**

D．推奨されるガイドライン

経営や運営に関する定期的な会議に報告できるように、比較的短いサイクルのプログラムも検討することが望ましい。

A．３．８　是正処置

A．JIS Q 15001：附属書A（管理策）

組織は、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、維持しなければならない。その手順には、次の事項を含めなければならない。 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、立案された適切な処置を実施する。 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。

B．保健医療福祉分野としての解釈

不適合は、パフォーマンス評価（A.3.7）の結果並びに緊急事態の発生、及び外部機関の指摘等により本規格の要求を満たしていないと判断したものである。不適合の原因が特定されなければ、根本的な解決にはならず再発を防げない。また、A.3.1.1 では、“各管理策の承認については、トップマネジメントによって権限を与えられた者によって承認されなければならない”としているが、保健医療福祉分野においては、患者等の個人情報を取り扱うため、不適合の内容によっては、その特殊性を十分に勘案したうえで是正処置を実施する必要があることから、被監査部門は、不適合の原因を特定した上で、再発防止のための是正処置を立案し、トップマネジメントの承認を受け実施しなければならない。最終的に不適合に伴うリスクは、トップマネジメント（医療法人の場合は理事長又は院長）が負うこととなる。是正処置を確実に実施させるために期限を区切ることは有効であるが、不適合の内容によっては、長期にわたることもあり得る。不適合の内容に相応した期限の設定をすることも必要である。

C．最低限のガイドライン

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。

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）

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。

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。

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)。

→付録14　是正処置及び予防処置実施記録の様式例

以上