医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版（案）に対する意見と考え方

●意見募集期間：令和５年４月19日（水）～同年５月18日（木）
●提出意見総数：15件（個人 13件、法人・団体 ２件）
※提出意見数は、意見提出者数としています。

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
1	個人	個人	01全般	0	全般	PDF形式なので閲覧しやすいように、ガイドラインとFAQともに、目次からのページへのリンク設定をしていただきたい。	ご意見を踏まえて、ガイドライン及びFAQについて、目次から各ページへのリンクを作成しました。		
2	個人	個人	02GL	13	3.1.1	善管注意義務については、もともと曖昧な言葉であることから脚注で良いので正式名称または本文書での定義を示すべきである。	「善管注意義務」は法律用語として一般的であり、また、本ガイドラインでは通常の用法で用いているため、改めて定義等を示す必要はないものと考えますが、頂いたご意見は今後の検討にあたっての参考とさせていただきます。		
3	個人	個人	02GL	38	5.1.6	また、個人情報を格納する記憶媒体の管理方法では、昨今地方公共団体でインシデントが現に発生していることから「敷地外への持ち出し禁止」の文言・文意を追加すべきである。	「5.1.1.リスク特定」の「表5-1 医療情報システム等提供上の代表的な脅威」として「機器や記憶媒体の持ち出し時の紛失・盗難」を挙げており、改めてご指摘の文言・文意を追加する必要は無いものと考えますが、頂いたご意見は今後の検討にあたっての参考とさせていただきます。 なお、個人情報を格納する記憶媒体の管理に当たっては、こうしたリスクを踏まえて運用管理規程が作成されるべきと考えます。		
4	個人	個人	FAQ	1	1.1	FAQ1.1には 製品の納入をもってその後の保守管理もなく売買契約が完了した場合は、本ガイドラインの対象範囲外、また、製品保証としてセキュリティパッチの提供等のみを行っている事業者は、本ガイドラインの対象範囲外とありますが、保守契約を締結するなどしてセキュリティパッチの提供等を行う事業者は本ガイドラインの対象となるのでしょうか？	保守契約を締結している場合は、本ガイドラインの対象となります。		
5	個人	個人	FAQ	6	4.2	FAQ案の「4.2 プライバシーマーク認定/ISMS認証の取得と本ガイドラインとの関係の考え方は？」に「適格性を示すことができる場合」とありますが、適格性を示すには何が必要でしょうか。 認定基準や適用範囲が同等であれば適格性があると考えられるでしょうか。 例えば、一般財団法人 日本品質保証機構によるJIS Q 15001 認証サービスは、プライバシーマーク認証と同様の認定基準（JIS Q 15001）ですが、プライバシーマークが法人単位で取得するのに対し、任意の単位で取得可能となっているため、組織全体を適用範囲としている場合には適格性があると考えられないでしょうか。 一般財団法人 日本品質保証機構　JIS Q 15001（個人情報保護） https://www.jqa.jp/service_list/management/service/jisq15001/	プライバシーマーク認定やISMS認証は、医療情報に限らず、個人情報の取扱いに関し、適切な体制を整備していることを示すものです。今般の改訂で、同等の第三者認証等として「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 3 年 3 月 30 日各府省情報化統括責任者（CIO）連絡会議決定）で示されている「クラウドセキュリティ認証等」を追加しましたが、現時点ではこれ以外の認証等は同等のものとして認めておりません。同等の第三者認証等については、頂いたご意見も参考としつつ、必要に応じて見直しを行ってまいります。		
6	個人	個人	02GL	24	4.4	「4.4. 第三者認証等の取得に係る要件」に「プライバシーマーク認定やISMS認証と同等の第三者認証等（表4-1参照）を示すことができる場合」と記載がありますが、プライバシーマーク認定にも同等の第三者認証があり、それを示すことができる場合、これに代えることはできないでしょうか。 例えば、一般財団法人 日本品質保証機構によるJIS Q 15001 認証サービスは、プライバシーマーク認証と同様の認定基準（JIS Q 15001）ですが、プライバシーマークが法人単位で取得するのに対し、任意の単位で取得可能となっているため、組織全体を適用範囲としている場合には同等であると考えられます。 一般財団法人 日本品質保証機構　JIS Q 15001（個人情報保護） https://www.jqa.jp/service_list/management/service/jisq15001/	同上		
7	医療 ISAC	団体	02GL	35	5.1.6	厚生労働省「医療情報システムの安全管理に関するガイドライン第６版」との平仄合わせを目的としたアップデートという観点から、半田町立病院のレポートを参照する立て付けは、今後の医療情報システム事業者/医療機関とのリスクコミュニケーションを促進する上でも、非常に良いと思います。 ただ、他の方もパブコメ提示していると思いますが、今回大きく見直しが行われた範囲について、寡聞ながら、官公庁が一定の法的拘束力を持って公表するガイドラインで、【コラム】という章（5.1.6 リスクコミュニケーション / p35)における作文が存在することにはさすがに驚きました。 そのため、p35の【コラム】とはガイドラインにおいてどのような位置づけを示すのか、明記していただきたい。 単なる「検討委員の茶飲み話」の位置付けで、「ああなんかいっているな」程度に事業者は受け取ればいいのでしょうか？それとも、ガイドラインの中にある以上、何らかの拘束力のある内容なのでしょうか？？ 忌憚なく言わせていただくと、もう少し、医療分野におけるセキュリティガイドラインの内容・構成の重要性・インパクトを真面目に考えていただきたいです。 本来的には、<リスクコミュニケーションの不備例>という記載をすべきではないでしょうか？いずれにせよ、【コラム】とは一体どのような意図で記載しているのか、まずその背景・認識を教えていただきたいです。経産省・総務省の認識として、半田病院の事案は【コラム】レベルでお茶のみトーク感覚で扱われるものでしかないという認識であれば、その旨を明示すべきと思います。その認識に国内の事業者は従いますので。	本項目は、「本ガイドラインに具体例が少なくわかりにくい」という事業者の皆様のご意見を受けまして、リスクコミュニケーションが不足した例として、「徳島県つるぎ町立半田病院」の事例を挙げることで、事業者の皆様にわかりやすくお示しすることを目的としております。		
8	個人	個人	FAQ	1	1.2	医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドラインFAQ（案）に対する意見となります。 P1　注釈 一読して分かり難いので、下記のように注釈を分けてはどうでしょうか （修正前）1 ここにいう「ＰＨＲ」は、「生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）」（総務省、厚生労働省、経済産業省「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」（令和３年4月））をいいます。 （修正後）1 ここにいう「ＰＨＲ」は、「生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）」2 をいいます。 2　総務省、厚生労働省、経済産業省「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」（令和３年4 月）	参考意見として承りました。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
9	個人	個人	FAQ	2	1.2	P2　本文 一読して分かり難いので、下記の表現してはどうでしょうか。 （修正前）・・・、既に他のPHR が格納されているPHR サービスに取り込む場合、全体として本ガイドラインの対象となります。 （修正後）・・・、既に他のPHR が格納されているPHR サービスに取り込む場合、データを取り込んだPHRサービス全体が本ガイドラインの対象となります。	ご意見を踏まえて記載を見直しました。	「受け取ったデータを、既に他のPHR が格納されているPHR サービスに取り込む場合、全体として本ガイドラインの対象となります。」	「受け取った医療情報を、既に他のPHRが格納されているPHR サービスに取り込む場合、医療情報を取り込んだPHRサービス全体が本ガイドラインの対象となります。」
10	個人	個人	02GL	11	2.2.3	医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1 版（案）のp.11(17 of 64)に記載のある、脚注12に関する意見です。 図2-6を見る限り、事業者Bはインフラを提供する事業者(IaaS)であり、PACS(画像システム)を提供することは無いかと思います。 IaaSは仮想化技術を利用してハードウェアリソース（CPU／メモリ／ストレージ）などのデジタルインフラをインターネット経由で提供するサービスと理解しています。 ご検討のほど宜しくお願い致します。	「2.2.3.医療機関等が複数事業者と契約するケース」の本文、図及び脚注は、あくまでも当該ケースを例示するためのものです。そのため、インフラを提供する事業者が、実際にPACSを提供することがあるかについて判断しているものではありません。		
11	個人	個人	01全般	0	全般	2000文字の文字制限のため、分割して提出します。1つめ 1.配布されるPDFの文書は、最低でもしおり付きPDFにして、可能でしたらWordの原ファイル(変更履歴付き)を公開することでレビューの質の向上、効率向上が期待できます。また、英国などでは政府が国民のためにPDFを公開することを禁止していると認識しています。ともかく見られて改竄されにくく、アナログ(紙)の延長であるPDFでの安易な提供に関して、本当に国民のための方法になっているかを個々の行政機関でも考えていって欲しいと思います。国民の1人としての意見として、しおり無しのＰＤＦは最低であり、Wordでの検索機能、変更履歴表示機能など非常に効果的、効率的、高品質でのレビューが可能です。利活用にあたり、資料作成するのにＰＤＦからのコピーペーストをして体裁を整えてなど非常に非効率な作業を実施しています。 本当は、NativeなHTML又はXML＋Readerなどの構成もいいのではないかと思います。	今後の検討にあたっての参考とさせていただきます。		
12	個人	個人	02GL	0	全般	2.「もしくは」の使い方 図2-2他で「もしくは」と使用している箇所が散見される。しかし、法文、公用文、契約書、JIS等において、1階層の場合は「又は」を使用し、「“又は”を用いて並列した項目、条件などの中を、更に小さく選択する項目、条件などを併記する場合には、その接続に“若しくは”を用いる。」ルールになっている。本書は公用文、法文でないため、厳格には従うことが必須ではないが、できるだけ誤解を招かないために、さらに、特別な合理的な理由がない限りは、そのルールに従うことが望ましいと考えます。漢字を使うかひらがなを使うかは、それ以外の漢字、ひらがなのバランスで適切に使い分けていいのではないかと思います。 また、助詞の「や」は、「及び」又は「又は」のどちらを表すか不明確になりやすいためJISでは使用を禁止している。本書はJISではないが、不明確になりやすい部分をできるだけ減らすため、合理的な理由がない限り、そのルールに準じたほうがいいかと思います。 (1)P25図5-1内 2箇所 (2)P27 表5-1内 「？不正に書き換える、もしくは破壊する。」 (3)P38（ケ） 「？資料の提供もしくは、医療機関等に代わり？」 (4)P38（コ） 「監査の方針や内容もしくは、監査に代替する対応？」 助詞の「や」は「及び」又は「又は」のどちらを表すか不明確になりやすいため使用をさける。 （変更案）「監査の方針及び内容又は、監査に代替する対応？」 (5)P45 「契約終了フェーズにおける情報流の特定例」の表内の「廃棄もしくは移管する」 (6)P46 「契約終了フェーズにおける情報流の特定例」の表内の「廃棄もしくは移管する」 (7)P47 「契約終了フェーズにおける情報流の特定例」の表内の「廃棄もしくは移管する」 (7)P54 「用語集」の「１ｏＴ」の説明内に2箇所	ご指摘を踏まえて修正いたしました。		（記述を修正）
13	個人	個人	02GL	2	1.1.2	3.P2 1.1.2医療法との関係 「また、医療情報安全管理ガイドラインは、健康保険法等に基づく健康保険制度の保険診療点数表において引用されており、保険医療機関としても遵守が求められている。」と記載されている。2023年3月10日付けで医療法施行規則第14条2項が新設され、病院、診療所又は助産所の管理者 が遵守すべき事項として、 医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じることを追加され、4月1日から施行されることが告示された。また、病院、診療所及び助産所におかれては、規則第1 4条第２項に規定する「必要な措置」として、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について 適切な対応を行うこととされた。このような観点でも医療機関等が医療情報安全管理ガイドラインを遵守する必要があることを明記したらどうかと思います。	医療機関等の医療情報安全管理ガイドライン遵守の必要性については、「1.1.2　医療情報安全管理ガイドライン」に記載しておりますので、原案通りとさせていただきます。		
14	個人	個人	02GL	2	1.1.3	59522302600000009の続き 2つ目 4.P2 1.1.3医療情報システム・サービス 「医療情報を取り扱う情報システムやサービス（以下、「医療情報システム等」という。）を提供する事業者」と記載されていますが、非常に誤解を招く表現になってしまっていると思われます。まず、助詞の「や」はJISでは、「及び」又は「又は」のどちらを表すのかが不明確になるため使用を禁止しています。また、本書のタイトルである医療情報を取り扱う情報システム・サービスの提供事業者の中点「・」も非常にわかりにくいと思われます。前回のパブコメでの回答では「医療情報を受託する情報処理事業者の安全管理ガイドライン改定検討会で議論されたもの」とのことで変更がなされませんでした。タイトルの変更は、関係者が多く簡単に変更できないことは理解できますが、1. 1.3の記載に関しては、もう少し誤解をうけない表現にすべきではないでしょうか。 (1) 情報システムを提供し、サービスを提供しない事業者は対象外 (2) 情報システムを提供し、サービスを提供する事業者は対象 (3) 情報システムを提供しないが、サービスを提供する事業者は対象 さらに、下記の変更案によって、現在のタイトルでの誤解を招く表現であることも、タイトルの変更なしに改善できるのではないかと思います。 (変更案) 「医療情報を取り扱う情報システムを用いたサービスを提供する事業者」（以下、「医療情報を取り扱う情報システム・サービスの提供事業者」という。）	「医療情報を取り扱う情報システムやサービス（以下、「医療情報システム等」という。）を提供する事業者」という表現につきましては、本ガイドライン統合時の検討会にて議論されたものであるため原案通りとさせていただきますが、頂いたご意見は今後の検討にあたっての参考とさせていただきます。		
15	個人	個人	別紙2	0	全般	5.P5 1. 3別紙2旧ガイドラインにおける対策項目一覧と医療情報安全管理ガイドラインの対応表 前版においては、この記載で問題ないとは思いますが、今回の版では「旧ガイドライン」が2世代前のガイドラインを指すので、最新のガイドラインを読む読者にとってはわかりにくいと思われます。また、医療情報安全管理ガイドラインも改訂されているため、対応も正確性を欠いているのではないかと思います。 提案として、別紙2のタイトルを「対策項目の具体的一例の一覧と医療情報安全管理ガイドラインの対応表」と変更し、最新の医療情報安全管理ガイドラインと、陳腐化してしまっている具体的対策を改訂するのがいいのではと思います。特に安全管理ガイドライン第6版においては、4編構成になりC項、D項がなくなっているため、別紙2を適切に更新できるように厚労省とも連携して欲しい。	ご意見を踏まえて、別紙２について、医療情報安全管理ガイドライン第6.0版に対応した内容に修正の上、名称を「別紙2統合前ガイドラインにおける対策項目一覧と医療情報安全管理ガイドライン6.0版の対応表」に変更しております。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
16	個人	個人	02GL	7	2.2	6.P7 2.2ぶらさがり段落(hanging paragraph) 2.2.1章が存在するときに、2.2章のタイトルの直下に文章を書くことは、「ぶら下がり段落」とよび、JIS(日本産業規格)では禁止されている文書構成である。本書がJISではないので、厳密には従う必要はないが、特別な合理的理由がない限り、従うのが望ましいと思います。2.2のタイトル内容に対して、2.2.1?2.2.3は、ケースを記載している。細分箇条にするのではなく、JISの言葉では細別(一般的には箇条書き)で(1)(2)(3)で記載したほうがいいのではないかと思います。	2.2直下に記載されている段落は、2.2.1-2.2.3が医療情報システム等の代表的な提供形態を類型化したものであることを述べた総論として記載したものである点、ご理解ください。		
17	個人	個人	02GL	11	2.2.3	7.P11 2.2.3 医療情報を直接扱わない事業者 2.2.3の構成において、「対象事業者A、対象事業者B はそれぞれ独立して自社の医療情報システム等について本ガイドラインに基づくリスクマネジメント及び制度上の要求事項への対応を行い」と記載されている。責任範囲の観点では、事業者A、事業者B及び医療機関等に関しては記載通りかと思います。しかし、事業者Bは自身では医療情報を取扱わない場合が多く、そのような場合では本ガイドラインの対象外との考えもできる。インフラの責任はあるが、本ガイドラインの対象外になる可能性がある。そのような場合に事業者Ｂの責任をガイドライン等で明確に定義する必要があるのではないかと思います。同様に自身では医療情報を直接扱わないプラットフォームを提供する事業者でかつ、直接医療機関等と契約する事業者についても考慮が必要ではないかと思われます。	本ガイドラインが対象とする事業者は「医療機関等との契約等に基づいて医療情報システム等を提供する事業者」となりますので、ご指摘の「自身では」の意味するところが定かではありませんが、「医療情報を取扱わない場合」には原則として本ガイドラインの対象外となります。他方で、ご指摘の2.2.3.図2-6に示す対象事業者Bにつきましては、同事業者が提供する通信回線等のインフラは「医療情報システム等」の一部ですので、医療情報を取扱う事業者となります。 なお、ご提示の考え方については、今後の検討にあたっての参考とさせていただきます。		
18	個人	個人	02GL	26	5.1.1	595223026000000010のつづき 3つめ 8.P26 5.1.1 リスク特定 「対象事業者は、自らが提供する医療情報システム等の全体構成図を作成することで、医療情報システム等の全体構成を明らかにすること。」と記載されている。この記載は対象事業者の責任範囲においては最低限の部分であり、これ以上にして医療機関と責任を共有できるようにしたほうがいいのではないかと思います。例えば、医療情報システムをクラウドで提供する事業者においては、クラウド内が責任範囲である場合が多いが、医療機関等からクラウドに接続するための機器、ネットワークも含めて構成図も誰かしらが書いておく必要がある。医療機関等が記載できれば問題ないが、それを期待するだけでなく冗長でも対象事業者も記載すべきではないかと思います。これにより5.2.1に記載の「この場合、全体構成図の作成に関する役割等を医療機関等と合意すること」とも整合が取れた記載になるのではないかと思います。 (変更案)「対象事業者は、自らが提供する医療情報システム等並びに必要に応じてその医療情報システム等を使用する環境及び関連する他のシステム等を記載した全体構成図を作成し、医療情報システム等の全体構成を明らかにすること。その医療情報システム等を使用する環境及び関連する他のシステム等は、必要に応じて医療機関等とのコミュニケーションを図り作成すること。」	（全体構成図を作成する目的である）構成要素間での情報流を洗い出す際には、「特に、医療情報システム等をクラウドサービスとして提供するケースにおいては、ASP・SaaS と PaaS、IaaS をそれぞれ別の事業者が提供する等、ICT サプライチェーンが複雑となる傾向にあるため、抜け漏れがないよう十分留意すること」としております。ご指摘の事項はこの具体的な方法に関するものと認識しておりますが、（今般の改訂において「全体構成図の作成に関する役割等を医療機関等と合意すること」という規定を追記したところ、）ガイドラインにおいてどこまで具体的に記載すべきかという点も含め、今後の検討課題とさせていただきます。		
19	個人	個人	02GL	54	用語集	9.P54 MACアドレス 「原則同一の MACアドレスを持つ LAN カードが 2 つ以上存在することはない。」と記載されている。原則はその通りですが、悪意を持ってとか他の要因で任意の値にすることが可能であるような記載を追記しておいたほうがいいのではと思います。	本項目は「用語集」であるため、「原則」を記載しております。		
20	個人	個人	02GL	2	1.1.2	10.P2 1.1.2「令和4 年●月には第6.0 版が策定された。 「令和4 年●月には第6.0 版が策定された。」と記載されている。まだ最終版が公開されていないので、変更があることは認識しているが、令和4年は明らかに間違いで少なくても令和5年。	ご意見を踏まえて、記載を修正するとともに、医療情報安全管理ガイドライン第6.0版の公表月を反映いたしました。	「令和4年●月には第6.0 版が策定された。」	「令和5年5月には第6.0 版が策定された。」
21	個人	個人	02GL	7	2.2	11.P7 2.2ぶらさがり段落(hanging paragraph) 3.1章が存在するときに、3章のタイトルの直下に文章を書くことは、「ぶら下がり段落」とよび、JIS(日本産業規格)では禁止されている文書構成である。できるだけそのルールに従うほうがわかりやすくなるのではないか。	3直下に記載されている段落は、3.1.3-2の総論として記載したものである点、ご理解ください。		
22	個人	個人	02GL	7	2.2	12.P7 2.2 「医療情報システム等の代表的な提供形態」 クラウドの利活用が増加しているため、記載の通りに複数の事業者が関与する場合の説明は非常に有効だと思われます。それだけではなく、医療機関内のネットワークとの関係の類型等も追加して記載してあるといいと思われます。通常、クラウド事業者は、医療施設とクラウドとの間のネットワークから責任を持つ場合が多いが、医療施設側の接続点(具体的にはVPN機器)、医療施設内の端末からVPN機器への経路設定、Zone,フィルタなどの変更などを医療機関が責任を持つことがもれる場合が多い。この部分をクラウド事業者が主になり、責任分界が明確にし、医療機関が知識、経験がない場合はそれへの適切な助言を明確に要件化するようにしたほうがいいと思われます。	参考意見として承りました。		
23	個人	個人	02GL	25	図5-1	13.P25 図5-1 リスクマネジメントのプロセス 図内で「5.1.5. リスク対応の実施手順」と記載されているが、5.1.5のタイトルは「リスク対応策の設計・評価」となっておりあっていない。どちらかに合わせるべきではないか。	ご意見を踏まえて修正いたしました。	「5.1.5.リスク対応の実施手順」	「5.1.5.リスク対応策の設計・評価」
24	個人	個人	02GL	27	表5-1	14.P27 表5-1 情報の改竄・破壊又は医療情報システム等の停止になるのかもしれませんが、最近のランサム(医療情報を暗号化され、医療情報システムが使用不能になり、身代金を要求)に関しても明示的に脅威として追加したほうがいいのではないか。	ご意見を踏まえて修正いたしました。	(追記)	「ランサムウェア感染□ 医療情報システム等や関連する端末等をマルウェアに感染させ、PCをロックする、あるいはファイルを暗号化することによって使用不能にしたのち、その復元と引き換えに身代金を要求する。」
25	個人	個人	02GL	29	5.1.4	15.P29 5.1.4 リスク管理方針（リスクの回避・低減・移転・受容）」と記載されている。最新のISO27000シリーズの記載においては、以前の定義であるリスク移転に代わり、リスク共有と定義されているため修正すべきではないでしょうか。	ご意見を踏まえて修正いたしました。		(記述を修正)
26	個人	個人	FAQ	6	5.2	595223026000000011のつづき 4つめ FAQ 16.P6 5.2 「5.1.5. リスク対応の実施手順」と記載されているが、ガイドラインの5.1.5は「リスク対応策の設計・評価」である。	ご意見を踏まえて修正いたしました。	「5.1.5.リスク対応の実施手順」	「5.1.5リスク対応策の設計・評価」
27	個人	個人	FAQ	4	2.2	17.P4 2.2. 「なお、医療情報連携ネットワーク運営主体の中には、医療情報に関する管理責任は負わず、参加団体の取りまとめや情報システム仕様の調整等のみを行っている者もあり、そのような運営主体については、本ガイドラインにおける対象事業者とはなりません。」と記載されていますが、「医療情報に関する管理責任を負わずに情報システム仕様の調整等」を言葉通りならばその通りなのかもしれません。しかし、管理責任を負わずに、情報システム仕様の調整等を行うことは、責任範囲が不明確になる可能性があるのではないかと思います。また、「参加団体のとりまとめ」に関しても、参加に関して医療情報の取扱い等含めて合意、契約等が必要になる可能性も否定できないかと思います。これらのため、記載方法等をもう少し考慮されてもいいのではないかと思います。	参考意見として承りました。ネットワーク運営主体が医療情報に関する管理責任等を負わない場合については対象外であるという趣旨でありますので、原案通りとさせていただきます。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
28	個人	個人	02GL	6	2.1	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版（案）」 6ページ目の注釈11に、「患者等から直接医療情報を受領する事業者は、本ガイドラインにおける対象事業者にはあたらない。」とあります。 本ガイドラインが対象とする同ページ内2.1で定義され解説されている医療情報は、健康診断、遺伝子検査結果、診療情報等を含む要配慮個人情報でもあり、医療DXなども見据えると、医療情報を扱う事業者における適切な管理が必要な情報です。 そのため、医療機関等又は患者等、医療情報の提供元によらず、医療情報を扱う事業者は本ガイドラインの対象としたほうがよいと思います。	今後の検討にあたっての参考とさせていただきます。		
29	個人	個人	02GL	24	4.3 4.4	＜項番１＞ ＜対象文書＞ガイドライン１．１　本文 ＜該当箇所＞P２４の４．３および４．４ ＜意見内容＞それぞれのタイトルを以下のように追加・修正する。 ４．３　医療情報システムの安全管理水準に係る評価 ４．４　提供事業者の体制の適格性を評価する第三者認証等の取得に係る要件 ＜理由＞本文のP２４の４．４の主旨や注２６の主旨やFAQのP5の４．２の説明の主旨を反映して、２つの評価を明確に区別して理解できるようにする為。	4.3は医療情報システム等の安全管理に係る評価を確実に行うことを求めており、その１つとして第三者認証で明示することを求めているものが4.4です。4.4も体制の問題だけではなく、適格性の第三者認証という趣旨になります。そのため、4.3については原案通りとさせていただき、4.4については、「対象事業者の適格性を評価する第三者認証の取得に係る要件」に修正いたしました。	「4.4.提供事業者の体制の適格性を評価する第三者認証等の取得に係る要件」	「4.4.対象事業者の適格性を評価する第三者認証等の取得に係る要件」
30	個人	個人	FAQ	1	1.2	＜対象文書＞FAQ ＜該当箇所＞P2　「２．医療情報システム等の提供形態」の前 ＜意見内容＞PHRに関する文章を以下に置き換える。（現在のPHRに関する説明は削除する） PHR事業者についても、患者等の指示に基づいて、医療機関等から送付された医療情報 を受け取る場合には、本ガイドラインの対象となります。 受け取ったデータを、既に他の PHRが格納されている PHRサービスに取り込む場合、全体として本ガイドラインの対象 となります。 「医療機関等から送付された医療情報」ではなく、「医療機関等から患者等に送付さ れた医療情報」に該当する場合（注１）は本ガイドラインの対象とはなりません。 また、健診等情報（注２）を取り扱うPHRサービスを提供する事業者が遵守すべき事項を示すものとして、 「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」（令和３年4月）（総務省、厚生労働省、経済産業省）があります。 （注１）例えば、医療機関等から患者等に対して、医 療情報を閲覧するための URL や QR コードの提供を受け、患者等がその内容を自ら PHRサービスに登録する場合などは、「医療機関等から患者等に送付された医療情報」に該当するため、そのような PHRサービスは本ガイドラインの対象とはなりません。 （注２）健診等情報は以下の情報を対象としている。 ・個人がマイナポータルAPI 等を活用して入手可能な健康診断等の情報 ・医療機関等から個人に提供され、個人が自ら入力する情報 ・個人が自ら測定又は記録を行うものであって、医療機関等に提供する情報 ＜理由＞ ３省のPHR指針は健診等情報に対するものなので、注１）の説明を有効とすると狭い範囲のＰＨＲになってしまう。 PHRに関するこれまでのガイドラインを整理した。さらに今後、「電子版お薬手帳ガイドライン」との整理が必要になると思います。	今後の検討にあたっての参考とさせていただきます。		
31	個人	個人	02GL	22	4.1	コメント１ 表4-1は「情報提供すべき項目」なのに「？機器等が、国内法の適用を受けることを確保すること」という要求事項的な表現なのはおかしい。 「？機器等に対する、国内法の適用状況」などが正しい。	「保存された情報を格納する情報機器等が、国内法の適用を受けることを確保すること」は要求事項であることから、原案通りとさせていただきます。		
32	個人	個人	02GL	22	4.1	コメント２ 表4-1は「情報提供すべき項目」なのに「プライバシーマーク認定又はISMS認証を取得していること」という要求事項的な表現なのはおかしい。 「プライバシーマーク認定又はISMS認証の取得状況」などが正しい。	プライバシーマーク認定又はISMS認証の取得は要求事項であることから、原案通りとさせていただきます。		
33	個人	個人	02GL	22	4.1	コメント３ 表4-1では 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無」としてISMAP等が挙げられていますが、 実際に「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針　2022年（令和４年）12月28日」を見ると4.1の1)にて (1)ISO？27017による認証？ (2)JINSA？CSゴールドマーク (3)？FedRAMP が挙げられており、第1.1版（案）では「(1)ISO？27017による認証？」が抜けているようです、追記をお願いします。 なお厚生労働省も「「医療情報システムの安全管理に関するガイドライン　５．１版」に関するＱ＆Ａ」のQ-64にて、JISQ27017の認証などの認証を挙げています。	令和5年5月に公表された、「医療情報システムの安全管理に関するガイドライン」第6.0版においては、ISO/SEC27017についての記載がないことから、原案通りとさせていただきます。		
34	個人	個人	02GL	24	4.4	コメント４ 4.4章にてプライバシーマーク又はISMS認証が求められており、また表4-1でも認証取得状況に関する情報提供が求められています。 しかしISMS認証を取得するには、マネジメント体制を構築し更に内部監査などを経る必要があり、マネジメント体制構築後数か月（3か月、4か月、6か月など諸説あり）掛かるとされています。 従ってサービスイン直後にはISMS認証を取得していないのが常識です。 このようにサービスイン直後でISMS認証がない場合、表4-1ではどのように情報提供すればよいでしょうか。 ISMS認証の取得計画などの情報を提供するのが現実的と考えますが本当にそうか、別添2-1「？ＦＡＱ？」にて考えをお示しいただきたい。 「セキュリティクラウド認証等」にも同じ構図があると推察します。	ISMS認証やプライバシーマーク、もしくはそれと同等の第三者認定等の取得は必須としております。取得予定ということであれば、時期等をご説明いただく必要があります。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
35	亀田医療情報　株式会社	団体	02GL	31	5.1.5	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版（案）」P31 5.1.5.　リスク対応策の設計・評価 (1)リスク対応策の設計 (ア)基本的な考え方 「医療情報安全管理ガイドライン（第5版）」とあるが、現行の第5.2版が正しいのではないか、又は、第6版が正式に発効された場合どのようになるのか。	ご意見を踏まえて、「医療情報安全管理ガイドライン」に修正いたしました。	「医療情報安全管理ガイドライン（第５版）」	「医療情報安全管理ガイドライン」
36	亀田医療情報　株式会社	団体	02GL	33	5.1.5	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版（案）」P33 5.1.5.リスク対応策の設計・評価 6 事業継続計画の策定における考慮事項 医療情報システムを提供する医療機関等の事情がそれぞれ異なる毎に計画の策定をすることは、事業者の負担が大きいため、必須であるかのような表現ではなく、「可能な範囲で医療機関等が想定する医療の継続性の観点に配慮した計画にすることが望ましい。」等の表現へ変更していただきたい。	事業継続計画の策定においては、医療機関等が想定する医療の継続性の観点を入れることを必須としていますので、原案通りとさせていただきます。		
37	亀田医療情報　株式会社	団体	02GL	35	5.1.6	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版（案）」P35 5.1.6.リスクコミュニケーション （１）医療機関等とのリスクコミュニケーションの実施 「合意形成を行う行為」は必要だが、合意に至るまでには、双方がベースとなる環境、技術的部分等の共通理解がなければ合意に至ることは難しく、また、一方だけが情報提供するべきものでもない。医療情報システムの提供後も合意形成に努めていくことを前提に、従来通り「図る」がよい。	昨今のサイバー攻撃による被害を防ぐためのリスクコミュニケーションとして、合意形成を「図る」のみではなく、合意形成を「する」ことが必要と考えられますので、原案通りとさせていただきます。		
38	亀田医療情報　株式会社	団体	02GL	36	1.1.3	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版（案）」P35 【コラム：リスクコミュニケーション不足がサイバー攻撃による被害発生の一因となった例】 所轄官庁から発出するガイドラインは、特定の事案に誘導することなく、広く公平に国民全体、且つ、対象となる業界団体、企業などへ伝達する必要がある、行政が発行する指針であるという認識である。 「事例」として、多々発生している事案があるにも関わらず、特定の事案、特定の固有名詞「徳島県つるぎ町立半田病院」を記載することで、取り上げられた事例のみに誘導する記載は、ガイドライン（付属資料含む）で記載するべきではない。 コラムが必要であるならば、医療機関等、事業者を責任の主体とするのではなく、その行動に至る原因となる制度、啓発活動がどうであったかを論点とし、固有名詞を省いてQA、読本に記載するべきである。	本ガイドラインにおいて具体例が不足しているとの御意見があったことから、具体例としてより分かりやすく示すため、報告書が公表されており、かつ、様々な場で取り上げられている「徳島県つるぎ町立半田病院」の事例を記載したコラムを新設いたしました。そのため、原案通りとさせていただきます。		
39	個人	個人	02GL	6	2.1	ページ：6 原文：本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システム等を提供する事業者9（以下、「対象事業者」という。）である10。ただし、医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者や、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は本ガイドラインにおける対象事業者11となる。 意見/理由：医療情報システムや機器等を売買契約により医療機関に販売した場合に、付帯するこれらの医療情報システムに対する現地保守サービスおよびリモート保守サービスがガイドラインの対象として該当するのかどうかが不明確のため、明記を頂きたい。なお、現地保守サービスおよびリモート保守サービスの提供の際に、医療情報を積極的に取得する場面はないもの、見えてしまうなどの場面は想定される。	「医療情報システムに対する現地保守サービスおよびリモート保守サービス」を提供する事業者は、「医療機関等に提供する医療情報システム等に必要な資源や役務を提供する事業者」に該当するため、本ガイドラインの対象となります。なお、FAQ 1.1に記載のとおり、製品やソフトウェアの提供者で、製品保証としてセキュリティパッチの提供等のみを行っている事業者については、本ガイドラインの対象範囲外となります。		
40	個人	個人	02GL	6	2.1	本編のP6 2.1. 本ガイドラインが対象とする医療情報と事業者において、対象事業者について、FAQで記載されている具体的な事例を本編で記載したほうがより周知されるので検討して頂けないでしょうか？また、記載が難しい場合は、FAQの参照箇所へ誘導するような記載があればよいと存じます。	ご意見を踏まえて修正いたしました。	（追記）	「本ガイドラインが対象とする医療情報と事業者に関しては、別紙2－1「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドラインFAQ」の「1．ガイドラインの対象範囲」に示す例も参照すること。」
41	個人	個人	02GL	22	表4-1	本編P22 表 4-1 医療機関等へ情報提供すべき項目で「国内法の適用を受けること…。」とありますが、国内法の適用を受けることを確認することとありますが、 ・国外に機器等があっても国内法が適用できれば問題ないとの理解でよろしいでしょうか？ ・海外事業者の医療情報に関するサービス（分析など）を海外の機器等を介して利用する場合、例えば、契約等で国内法の適用が担保できれば確認が取れたことになりますでしょうか？	国外における個別のケースについて判断できませんが、法やガイドラインの趣旨に則って、各医療機関や事業者が円滑に事故調査に対応できる体制で医療情報システム等をご利用いただくことを求めております。		