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2.0版（案）に対する意見と回答

●意見募集期間：令和6年10月2日（水）～同年10月31日（木）
●提出意見総数：17件
※提出意見総数は、意見提出者数としています。

No.	資料	該当箇所	意見	回答
1	本体	1.2	上から２行目。「リスクコミュニケーション」の意味を注釈で説明してはどうでしょうか。後述の5.1.6で説明はされていますが、ここで出てくるのは時期尚早だと思われます。	1.2では本ガイドラインの策定方針の説明のため「リスクコミュニケーション」の語句を記載している点及び5.1.6に詳細を記載している点から、1.2での注釈は不要であると考えます。
2	本体	図	図の説明をすべて左寄せにすべきだと思われます。	図のタイトルは、本ガイドライン全体で中央揃えで統一させていただきました。
3	本体	図2-4	図の名称は「図2-6」ではないでしょうか。	e-govにて公開した案は正しい表記でしたが、総務省の報道発表にて公開した案に誤りがありました。
4	本体	2.2.3脚注	"･･･が提供する電子カルテシステムと 業対象事業Bが提供する PACS･･･"の「業」は不要ではないでしょうか	e-govにて公開した案は正しい表記でしたが、総務省の報道発表にて公開した案に誤りがありました。
5	本体	表4-1	「情報提供すべき項目」のP21の上から１枠目とP22の上から2及び３枠目は関連しているので、続けて記載してはどうでしょうか	御指摘を踏まえ、表中の項目を入れ替えました。
6	本体	表4-1	「情報提供すべき項目」P22上から２枠目が、P21の上から１枠目と記述が異なるので修正してはどうか （現在）医療情報を保存する情報機器が設置されている場所 地域, 国 （提案）医療情報を保存する情報機器等が設置されている場所 地域, 国"	御指摘を踏まえ、修正いたしました。
7	本体	4.4	上から３行目の表現を注釈２２の記述に合わせる。さらに、プライバシーマークは認定であるため。 （現在）･･･, 情報セキュリティに係る公的な第三者認証として、･･･ （提案）･･･, 情報セキュリティに係る公的な第三者による評価として、･･･	4.4のタイトルに合わせ、「情報セキュリティに係る公的な第三者認証等として」といたしました。
8	本体	4.4	上から６？１０行目の追加された説明は必要ないと思われます。 ISMSは認証の適用範囲がさまざまで、対象事業者全体や製品単体などで認証を受けます。しかし、ISMS認証の説明する際には、提供する医療情報システム等に関わる部分を中心にして行いますので、結局のところP20の４． １節で提供する情報で説明することになると思われます。あえて新しく準備を促すよりも、提供する資料で説明できるように促した方が良いと思われます。	新たな準備を促すという目的ではなく、適切な対策の実施及びその説明責任を促すことを目的として追記したものであり、原案のとおりとさせていただきます。
9	本体	5.1.1	"下から８行目で、ASPがクラウドサービスの一部と説明されていますが、用語集のP59「クラウドサービス」には含まれていません。矛盾していますので、下記のようにしてはどうでしょうか。 （現在）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･･･ （提案）特に、医療情報システム等をクラウドサービス等のインターネット経由で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･･	御指摘を踏まえ、「クラウドサービス等」に修正いたしました。
10	本体	表5-3	「リスク受容（リスク保有ともいう）」で２種類のフォントが使われています	御指摘を踏まえ、修正いたしました。
11	本体	用語集	ASPを単独で説明してはどうでしょうか。内容は下記となります。 （提案）インターネットを経由して、アプリケーションを提供するサービスです。シングルテナントで提供をしますので、クラウドサービスとは異なり、ユーザの要求に応じたアプリケーションのカスタマイズが可能となります。	ASPについては、必ずしもシングルテナントでの提供に限らない場合もあるため、原案のとおりとさせていただきます。
12	本体	6.	上から４行目 「事業者は医療機関等に対し別紙 2 を適宜参照する等して説明すべきである。」 の別紙２はどの文書を指しているのでしょうか？ FAQのP8の5.3.節で別紙 2 の説明が出ていますが、旧1.1版の別紙のように読み取れます。対策を参照する文書としては良いと思います。本紙を採用するのであれば、少なくとも題目を変更すべきではないでしょうか？総務経産省のガイドラインの統合を知らない旧当者が参照することも考慮すべきです。	別紙２は、「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」を指しています。また、当該別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。
13	FAQ	4.2	上から２行目；第三者認証の語句が使われていますが、プライバシーマークは「認定」です。下記の通りに修正してはいかがでしょうか （現在）に係る公的な第三者認証として、プライバシーマーク認定またはISMS 認証の取得を求め （提案）に係る公的な第三者の評価として、プライバシーマーク認定またはISMS 認証の取得を求め	ガイドライン本体の記載に合わせ、「第三者認証等として、プライバシーマーク認定またはISMS認証の取得を求め」に修正いたしました。
14	FAQ	4.2	下から１から２行目；前提案と同様です （現在）････同等の第三者認証等があり、･･･ （提案）････同等の第三者認の評価があり、･･･	ガイドライン本体の記載に合わせ、原案のとおりとさせていただきます。
15	FAQ	5.1	下から２行目医；リスク保有の語句が使われています。下記の通りに統一してはどうでしょうか。 （現在）････リスク共有やリスク保有を選択する･･･ （提案）････リスク共有やリスク受容を選択する･･･	御指摘を踏まえ、修正いたしました。
16	FAQ	5.3	別紙２の説明がかかれていますが、今回のパブコメの文書として提示されていません。題目が「統合前ガイドライン･･･」となっていますが、新しい文書として発行してはどうでしょうか。ガイドラインを統合したことを知らない新人の担当者が読む場合もあります。	別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。
17	SLA参考例	全体	サービスレベル合意書（SLA）は、対象事業者がサービスを提供する際の約款や利用契約の一部です。このため、合意を図る文書のレベルでの解説ではない方が良いと考えます。一方、サービス仕様適合開示書はサービスの詳細説明という位置づけになります。このため、記載の順番は、SLAの方が先に説明すべきと考えています。説明や記述の順番が常にサービス仕様適合開示書を先頭にすることに違和感があります。P3の第３段落にも「･･･、提供サービス内容として合意するために、サービス仕様適合開示書を添付し、SLA の内容とすることも想定される。」と書かれていますので、SLAの方が上位文書となると本書でも説明をしています。	本ガイドラインにおける合意のプロセスは、契約の前に、サービス仕様適合開示書による情報提供すべき内容を提示し、それを踏まえて、SLAを利用した合意形成を行うことを想定していることから、原案のとおりとさせていただきます。
18	SLA参考例	図2	図中央の右側の赤枠内に「要求仕様適合開示書」と書かれています。この文字はここでしか使われません。出所元の図の変更ができないのであれば、説明が必要と思われます。本書は「SLA」と「サービス仕様適合開示書」の内容が書かれているので、キーワードは正確に使うべきです。	御指摘を踏まえ、修正いたしました。
19	SLA参考例	2.(1)③	本サービスの提供時間ロ 保守業務に関する事前連絡等 医療機関側の法定停電に際に、サービスが利用できなくなる場合がある時は、この取り決めが必要であることの説明を追加してはどうでしょうか。例えば、法定停電の時間は提供時間に含まれない、停電再開後に保守作業が必要な場合は医療機関から法定停電があることの事前連絡を行う、などです。	P23の「解説」に記載している「定期保守等による停止」には、法定停電による停止も含むことを意図しておりますので、原案のとおりとさせていただきます。
20	本体	2.1	[意見対象] 2.1 「医療情報」の定義 [意見] 本ガイドラインの適用対象となる「医療情報」には、医薬品や医療機器等にかかる臨床試験に関する患者情報（個人識別情報）も含まれるとの理解でよいか。 [理由] 「医療情報」という用語を用いた場合、診察・治療において得た患者情報のみが含まれるかのように読め、患者をリクルートして医療機関において行われる臨床試験（いわゆる治験）に際して得られる患者情報は、含まれないようにも読めてしまうおそれがある。 [補足] ・ 臨床試験において得られる患者情報を保管・処理等するシステムとしては、電子カルテといった診療・治療においても使われる医療情報システムに限らず、治験専用のシステムも用いられる。本ガイドライン中には、臨床試験に関する記述が一切ないことも相まって、こうした治験専用のシステムについてあたかも本ガイドラインの適用な誤解をシステムベンダー（たとえば株式会社ＮＴＴデータもその例の一つ）や医療機関をするのを防ぐために、明記を求める次第。 ・ 立場上、匿名で意見を具申することご容赦いただきたい。	本ガイドラインでは、2.1に記載のとおり、「医療情報」を、「医療に関する患者情報（個人識別情報）を含む情報」と定義しています。この定義を満たす臨床試験に際して得られる患者情報についても、「医療情報」に該当します。
21	本体	2.1	[意見対象] 2.1 本ガイドラインが対象とする医療情報と事業者 「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」の意義 [意見] 企業主導治験において、医療機関に治験を依頼する治験依頼者が、治験において用いる医療情報システム等の利用費を負担する場合、この治験依頼者は「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」の類型に該当するという理解でよいかを本ガイドラインまたはFAQに明記いただきたい。 [理由] ・ 企業主導治験においては、企業（主に製薬企業）が医療機関に対して治験を依頼し、医療機関は、患者を募って治験を行う。そして、その際、通常の診療では用いない医療情報システム等を医療機関がシステムベンダーと契約して用いる場合がある。 ・ このような場合、契約関係としては、 （１）治験依頼者-医療機関の間の治験実施契約（GCP第13条） （２）医療機関-システムベンダー間のシステム利用契約（GCP第39条の2） （３）治験依頼者-医療機関-システムベンダー間において、上記（２）のシステム利用料は治験依頼者が負担する旨の契約 となることが多い。 実務上は、（２）と（３）を合わせて一つの契約とすることも多い。 ・ こうした場合、当該治験に必要な医療情報システム等については、治験依頼者はシステム利用料を負担するものの、治験依頼者自身は、当該システムベンダーへの委託元ではなく、また、当該システムベンダーに対する指示等を行うことが許されていない。 というのも、仮に治験依頼者がシステムベンダーに対して指示等を行えるとすれば、治験によって生じるデータを治験依頼者が自社に有利に改ざん等する懸念があるためであり、この懸念は、PMDAがつとに表明しているところである。 ・ 治験において一般的な契約形態は以上のとおりであるところ、「治験依頼者」につき、本ガイドラインの適用があるかは本ガイドライン上明らかではない。臨床開発や治験といった用語が本ガイドライン上に現れないこともこの点の不透明さを増す原因となっている。 ・ いわゆるDCTも含め、治験の分野にデジタル技術が活用される場面は増えてきて、治験において医療機関が外部のシステムと接続し、患者情報が連携される場面は増えていくことが予想されるため、治験依頼者への本ガイドラインの適用の有無及び義務の内容を明らかにしておくことが、医療機関と治験関係者の間の共通理解を深めるのに資すると考え伺う次第である。	治験を目的とする場合であっても、以下条件に照らして、本ガイドラインが対象とする事業者への該当性についてご判断いただく点は、他の目的と相違いことから、原案のとおりとさせていただきます。 ①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、 ②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 ③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

22	本体,FAQ	2.1,1.3	[意見対象] 2.1「本ガイドラインが対象とする医療情報と事業者」の「医療情報システム等の売買契約等のみであり、運用、管理、保守に関する契約等がない場合は、「契約等」に含まれない。」の意味 [意見] １） 売買契約を締結した場合、「担保の責任を負わない旨の特約」（民法第572条）を付さない限り、契約不適合責任（旧法下では瑕疵担保責任と呼ばれていたもの）を売主であるメーカーは負う。 かかる特約を付さなくとも、「運用、管理、保守に関する契約等がない場合」に該当するのか、またどのような特約を付した場合には本ガイドラインの適用がないことになるのかを明記していただきたい。 ２） FAQ案1.3に「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。」とあるが、製品保証として、売買契約締結後一定期間の修理・交換を無償でメーカーが製品保証として行っている場合も、本ガイドラインの対象範囲外となるとの理解でよいかを明記いただきたい。 [理由] 意見募集の対象となるガイドライン案及びFAQ案は従前よりも記載は明確化されているものの、必ずしも、適用対象かの判断が一律にはできない、しばしば、契約当事者の社内、また、医療機関及びシステムベンダー間で適用の有無が問題となることもあり、責任分界の議論といったような議論をする以前の段階で余計な確認・交渉手続が発生するのを今回の意見募集を機に減らすのが、本ガイドラインの目的にかなっていると考える。そのため、実務的な観点から本ガイドラインの適用の判断について迷う点をあらかじめ明確化すべく、お伺いする次第である。 具体的には、上記の意見は以下のような背景がある。 まず、日本の民法が適用される売買契約は、特約を結ばない限り、契約不適合責任を売主であるメーカーは負うものとされる。製品保証と契約不適合の関係は明確ではなく、メーカーの売買契約において、どのような特約が付されている場合、本ガイドラインの適用がないことになるのかを明らかにしておきたいと考える次第である。たとえば、「本売買契約における契約不適合責任は、適用ある法令上の義務に反しない限り、セキュリティパッチの提供又はそれに類する内容に限られるものとする。」との特約を付さない限り、本ガイドラインの適用があることになるのか、を確認したい。これが意見１の背景である。 次に、製品保証は明確な法的な定義がない概念であり、実際には、製品ごとに幅がある。そして、セキュリティパッチの提供に加えて、修理や点検といった内容も売買契約の際に製品保証として付されていることが多いとの実務的感触を弊職は持っている。FAQ案では、「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」という記載があるが、実際のところ、「医療情報システム等」の売買契約で製品保証がその程度にとどまる売買契約はかなり少ないものと思われる。そのため、「あくまで例外的な仮想事例として、もし仮にセキュリティパッチの提供又はそれに類する内容のみを製品保証とする売買契約があったとすれば、本ガイドライン対象範囲外になる」という意味とFAQ案は読むのが自然と考える。ただ、FAQ案の当該記載が、あくまで仮想事例であり、かつ、例外的な場合であるというニュアンスがFAQ案上からは読み取れないため、その点の確認を求めたいというのが意見２の背景である。	個別の契約に対する本ガイドラインへの該当性については、契約によって態様が異なることから、本ガイドライン上で網羅的に明記することは困難であり、事業者等により自らご判断いただく必要がございます。また、FAQ1.3は、あくまでも「セキュリティパッチの提供等のみを行っている事業者」が本ガイドラインの対象外であることを記載しているまでであり、一般の製品保証についてまで言及しているものではございません。
23	本体,FAQ	2.1,1.3	[意見対象] 2.1本ガイドラインが対象とする医療情報と事業者 FAQ案 1.3 「保守要員を医療機関等に派遣し、医療機関等の指示に基づいて保守を行うケース」の意味 [意見] 医療情報システム等の提供事業者が、医療機関等に自己の従業員を派遣し、派遣先の指示に基づいて当該従業員が保守を行う場合というのは、当該提供事業者が、労働者派遣法（通称）上の許可を得て、医療機関等に労働者派遣をしている場合を想定した記載か。趣旨を明確にしていただきたい。 [理由] 「保守要員を医療機関等に派遣し、医療機関等の指示に基づいて保守を行うケース」を文言上読むと、「自己の雇用する労働者を、当該雇用関係の下に、かつ、他人の指揮命令を受けて、当該他人のために労働に従事させること」（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律第2条1号）に該当し、当該事業者は、厚生労働大臣の許可（同法第5条第1項）が必要になる。 そのような形態の保守サービスの提供がありうることを否定するわけではないが、かなり特殊な形態と思われる。そこで、本ガイドラインがかかる労働者派遣の形態での保守の形態を想定して、その形態については本ガイドラインの適用はないと記載しているのかを確認したい。	ご認識のとおり、当該記載は、医療機関等に労働者派遣を行う場合に関するものです。いただいたご意見については、同様の趣旨を既に記載しておりますので、原案のとおりとさせていただきます。
24	全体	全体	1.該当箇所：全体 意見内容：今回、見え消し版、FAQ案、SLA(案)も同時に公開してくれて、非常に参考になります。 しかし、本文は、しおり付きのPDFにして頂けると、電子的な可読性が高まると思います。少なくても、正式発行の時は、本文はしおり付きPDFでSLAはWord版でも公開してほしい。	ご指摘を踏まえ、本ガイドラインについてしおり付きpdfで公開するとともに、SLA参考例についてword版での公開も行います。
25	本体	全体	2.該当箇所：全体 意見内容：本ガイドラインと、「医療情報システムの契約における当事者間の役割分担等に関する確認表」(総務省、厚生労働省、経済産業省)との関係を本ガイドラインで説明してほしい。 最低限としては、3章で参照してほしい。 今後は、事業者をシステム提供する事業者、システムを提供してその保守を実施する事業者、システムを元にサービスを提供する事業者のような特質に応じて、その責任が異なるため、前記ガイドラインと、本ガイドラインで実施すべきことなどを明確に規定してほしい。	「医療情報システムの契約における当事者間の役割分担等に関する確認表」の対象は、「2.本確認表の使い方」に記載のとおり、「マルチベンダー型契約により役割分担等が複雑であるものの、法務やITに精通した担当者が不在である中小規模の病院」を想定しており、対象となる病院が事業者との協議において項目の具体化を行うことを主目的としたツールの一つとして提供されているものです。したがって、当該確認表は、本ガイドラインを構成する資料ではないことから、本ガイドラインの中では位置づけの説明等は行いません。
26	本体	1.3	3.該当箇所：1.3 本ガイドラインの構成 （最後の文節） 意見内容：FAQ, SLAの案は、別紙として公開されたが、「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」は公開されていない。同時に公開されるのがいいのでは。 P7では、FAQを別紙2-1「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」」として参照している。別紙の構成も明確にしたほうがいいのでは。	「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」については、今回改定を行っておりません。 また、御指摘いただいたP7の「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」」の記載について、ここでの「別紙 2-1 」の記載は不要であることから、修正いたしました。
27	本体	2.1	4.該当箇所：2.1 本ガイドラインが対象とする医療情報と事業者 本ガイドラインが対象とする事業者は、？ 運用又は管理、保守に関する契約等がない場合は、「契約等」に含まれない。 意見内容：対象の範囲ですが、「医療情報システム等の売買契約等のみ」は含まれない。一方、売買契約等以外の契約があれば対象となるようにも読める。例えば、売買契約とともに、典型的な有体物(ハードウェア)の「清掃、校正（キャリブレーション）、消耗部品の交換等」の契約等があれば対象ともとらえられる。契約があるかどうかではなく、医療情報システムを用いたサービスを提供するかどうかで対象かどうかを判断するようにすべきではないかと思います。これにより、JAHIS/JIRAの「製造業者 /サービス事業者による医療情報セキュリティ開示書チェックリスト」のSDSの対象かどうかと整合がとれ、理解しやすくなるのではないかと思います。 例えば、クラウドの電子カルテの場合、いわゆるクラウドサービスとして提供するのか、オンプレミスとして提供するのかにより、事業者が実施すべき範囲と、医療機関等が実施すべき範囲が異なる。サービスとして提供する場合は、事業者が実施すべき範囲と提供すべき情報とが異なる。この内容は、今回の厚労省 安全管理ガイドライン第6版 概説編「３． ２． 医療機関等の特性に応じた 読み方」等で明確化されている。 (修正案) 「本ガイドラインが対象とする事業者は、1.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用いたサービスを提供する事業者 、2.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サービスや役務を提供する事業者、3.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 （以下、これらを総称して「対象事業者」という 。）である 1.における「医療機関等との契約等に基づいて」にある「契約等」に は 、医療情報システム等の運用又は管理、保守等のサービス に関する契約等が含まれる 。例えば 、医療機関等の外部において医療情報の保存等を行うサービス等の提供契約 も、「契約等」として挙げられる。しかし、医療情報システム等の売買契約等のみであり、運用又は管理、保守に関する契約等がない場合は、「契約等」に含まれない。	参考意見とさせていただきます。本ガイドラインの対象範囲の考え方については、FAQの1.に記載していることから、原案のとおりとさせていただきます。
28	本体	2.1	1.該当箇所：2.1 本ガイドラインが対象とする医療情報と事業者 「医療情報システム等 」には、？ 意見内容：ここで、契約等がどこまで含まれて、どこまで含まれないかが明確ではない。医療機器の保守点検は、医療法により、医療機関に義務づけられている。一般的に医療機器の文脈での"保守"とは、「清掃、校正（キャリブレーション）、消耗部品の交換等」で、"保守契約"とは、前記、保守と障害対応で、主にハードウェアの対応となっています。 さらにサイバーセキュリティにおいては、薬事法の基本要件基準改訂により、セキュリティに関するリスクマネジメント、保守時のリスクコミュニケーションが要求されています。 このような状況のため、もし、医療機器を本ガイドラインの対象とする場合は、２つの異なる要求を実施する必要が存在してしまう恐れがあります。特に、SLAに関しては、クラウド等のサービスに適した項目が多く、検査機器等の医療機器には適さない記載も多くあると思われます。 これらのため、医療機器当の場合は、契約等があるかどうかというより、それを用いたサービスを提供するか否かなどが、スコープを決める要素にしたほうがいいのではないかと考えます。 または、医療機器の場合は、前記の基本要件基準等で同等のことが要求されているので、本ガイドラインの対象外と明確に記載するのがいいのではないかと思います。	参考意見とさせていただきます。医療機器における本ガイドラインへの該当性については、FAQの1.に記載していることから、原案のとおりとさせていただきます。
29	本体	全体	2.該当箇所：(1) 2.2の直下の2.2.1の前まで (2) 3の直下の3.1の前まで (3) 3.2の直下の3.2.1の前まで (4) 4の直下の4.1の前まで (5) 5の直下の5.1の前まで (6) 5.1の直下の5.1.1の前まで (7) 5.2の直下の5.2.1の前まで (8) 6の直下で6.1の前まで 意見内容：例えば、2.2.1が存在するときに2.2の直下に文章を書くことをぶら下がり段落(hanging paragraph)といい、JIS, ISO, IECでは禁止している文書構成である。本書は、JIS等ではないので厳格に従う必要はないが、標準化等の文書で経験のあるJIS, ISO, IECに禁止されている文書構成は、適切な理由がない限り避けたほうがいいのではないか。	例えば、2.2は、2.2.1～2.2.3の記載全体について説明している記載であるため、原案のとおりとさせていただきます。
30	本体	5.1.5	3.該当箇所：5.1.5 (1)リスク対応策の設計・評価（ア)基本的な考え方 さらに、対策を設計する際に、別紙２に書かれている「対策項目で対応できるリスクシナリオ（例）」を参考にすることも有効である。 意見内容：(1)前回1.1版のパブコメにおいて、別紙2の名称は、「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」に変更されたのでは。 (2) 本来は、そのコメントのように、「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。」のとおりに対応した上で公表してほしい。 (3) (2)を実施することにより、本文記載の「参考することも有効」のようになるのではないかと考えます。	ご指摘の(1)について、別紙2の名称は、「1.3. 本ガイドラインの構成 」において、「「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」（以下、「別紙2」という。）」と記載させていただいております。 ご指摘の(2)(3)について、別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。
31	本体	用語集	4.該当箇所：用語集 脆弱性 脅威によって悪用される可能性がある欠陥や仕様上の問題。 意見内容：現状の用語の説明だと、「？欠陥」又は「？問題」となり、製造物の責任があるように誤解を与える。どのように設計、開発しても、出荷時にはわからなかった「脆弱性」が後から発見されることが普通である。その性質を抑えた上で、出荷してからの対応が望まれる。 このため、JISQ27000の用語の定義を使用したほうがいい。 (修正案) 一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。	当該記載は、脆弱性について製造物の責任のみよって生じるものであることを意味しておらず、実際に意図しない欠陥や問題によって生じ得ることから、原案のとおりとさせていただきます。
32	別紙２	全体	（１）：「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」が更新されていない理由は何か？別紙２の内容は、第1版が制定された2020年から変更がなく、別紙２に定められた対策のなかには古いものも含まれており、アップデートが必須と思われる。 5-1-5：リスク対応策の設計・評価(p38)において、「（･･･）対策項目として整理・統合した別紙 2を用い、その全ての対策項目について対応していることを確認すること は、対象事業者による対策の設計や妥当性の判断、説明義務への対応において必須である」と記載がある通り、事業者が医療機関に対して自社の取組を説明するには別紙2を用いることが推奨されている。しかし、2020年時点の要求事項への対応を2024年に説明されても実効性は乏しくおもわれる。 また、6：制度上の要求事項（p69)でも「医療情報安全管理ガイドラインにおける制度上の要求事項への対応策について、対象事業者は医療機関等に対し別紙 2 を適宜参照する等して説明すべきである」とあり、医療機関へ説明するための根拠資料として別紙２が参照されているかぎり、別紙１のみでなく、別紙2も更新すべきと考える。 クラウド事業者の多くは「別紙２」（2020年時点）への対応状況をまとめた資料をセキュリティリファレンスとして公開することが多い。別紙２を更新しないのであれば、別紙２はあくまで初版時点の最低限の対策内容をまとめたものであり、事業者は直近のリスク動向を鑑みてしっかりとしたリスク評価結果に基づく個別の追加対策の要否、そして実施状況についても、医療機関に説明する必要がある点を明記すべきと考える。	別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。

33	全体	全体	（2）：2024年6月に公開された「医療情報システムの契約における当事者間の役割分担等に関する確認表」が第2版の中でどのように位置づけられるかについても明記すべきと考える。 特に「別紙1　ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例（案）」との関係性を明確に整理頂きたい。 事業者によっては別紙１やMDS/SDSの提出をもって、リスクコミュニケーションを果たしたと勘違いするものもあり、そのため、確認表のような契約調整における着眼点を整理した重要な資料を単なる関連文書でなく、明確に第2版に組み込むべきと思料する。	「医療情報システムの契約における当事者間の役割分担等に関する確認表」の対象は、「2.本確認表の使い方」に記載のとおり、「マルチベンダー型契約により役割分担等が複雑であるものの、法務やITに精通した担当者が不在である中小規模の病院」を想定しており、対象となる病院が事業者との協議において項目の具体化を行うことを主目的としたツールの一つとして提供されているものです。したがいまして、当該確認表は、本ガイドラインを構成する資料ではないことから、本ガイドラインの中では位置づけの説明等は行いません。
34	全体	全体	[項番] 1 [該当箇所] 全体 [意見内容] 今回、見え消し版、FAQ案、SLA(案)も同時に公開してくれて、非常に参考になります。 しかし、本文は、しおり付きのPDFにして頂けると、電子的な可読性が高まると思います。少なくても、正式発行の時は、本文はしおり付きPDFでSLAはWord版でも公開していただきたい。 [理由] ガイドライン1.1のパブコメでも同様なコメントで、正式版ではしおり付きのPDFを公開してくれた。 https://www.soumu.go.jp/main_content/000891031.pdf	ご指摘を踏まえ、本ガイドラインについてしおり付きpdfで公開するとともに、SLA参考例についてword版での公開も行います。
35	本体	脚注22	[項番] 2 [該当箇所] P23脚注22 JIS Q 27001:2014 (ISO/IEC 27001:2013) に基づく認証 [意見内容] 具体的に当該ドキュメントを参照してない場合は、最新版を参照することを誘導するために年を書かない方がよいと思われる。 修正前：JIS Q 27001:2014 (ISO/IEC 27001:2013) に基づく認証 修正後：JIS Q 27001 (ISO/IEC 27001) に基づく認証 [理由] https://www.jsa.or.jp/ms-sp-1/jisq27001/	御指摘を踏まえ、修正いたしました。
36	本体	4.4	[項番] 3 [該当箇所] P24「保健医療福祉分野のプライバシーマーク認定指針（第 4 .1 版）」を参照し、 [意見内容] 具体的に当該ドキュメントを参照してない場合は、最新版を参照することを誘導するために版を書かない方がよいと思われる。 修正前：「保健医療福祉分野のプライバシーマーク認定指針（第 4 .1 版）」を参照し、 修正後：「保健医療福祉分野のプライバシーマーク認定指針 」を参照し、 [理由] https://privacy.medis.or.jp/shishin5.html	御指摘を踏まえ、修正いたしました。
37	本体	1.3	[項番] 4 [該当箇所] P5 1.3 活用することを想定した「別紙 1 サービス仕様適合開示書及び SLA の参考例」（以下、「別紙 1 」という。）及び第 5 章に基づくリスクマネジメントの実践に おいて事業者 が 確認する 内容として、「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」（以下、「別紙 2 」という。）を用意している。 [意見内容] FAQ, SLAの案は、別紙として公開されたが、「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」は公開されていない。 本文に書いてある別紙2は最新化された別紙2を提供していただきたい。	別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。
38	本体	脚注14	[項番] 5 [該当箇所] P14 3.1.2 脚注14 より改正民法に対応した「情報システム・モデル 取引・契約書」 https://www.ipa.go.jp/digital/model/model20191224.html [意見内容] リンク切れのため、下記に更新要 https://www.ipa.go.jp/digital/model/model20201222.html	御指摘を踏まえ、修正いたしました。
39	本体	表4-1	[項番] 6 [該当箇所] P21 表4-1 ・Certified Information Systems Audito （ISACA認定） [意見内容] 誤植 Auditorの最後のrが抜けてしまっている。	御指摘を踏まえ、修正いたしました。
40	本体	脚注22	[項番] 7 [該当箇所] P23 4.4 脚注22 ISMSに関する一般的な基準である JIS Q 27001:2014 (ISO/IEC 27001:2013) [意見内容] 具体的に当該ドキュメントを参照してない場合は、最新版を参照することを誘導するために年を書かない方がよいと思われる。 修正前：ISMSに関する一般的な基準である JIS Q 27001:2014 (ISO/IEC 27001:2013) 修正後：ISMSに関する一般的な基準である JIS Q 27001 (ISO/IEC 27001)	御指摘を踏まえ、修正いたしました。
41	本体	5.1.4	[項番] 8 [該当箇所] P30 5.1.4 なお 、対象事業者の判断のみによってリスク 共有 やリスク保有を選択することは適当ではなく、医療機関等への説明や合意形成の上、これを選択 [意見内容] 更新漏れと思われる なお 、対象事業者の判断のみによってリスク 共有 やリスク受容を選択することは適当ではなく、医療機関等への説明や合意形成の上、これを選択 [理由] 最新のISMSの用語とすべき	御指摘を踏まえ、修正いたしました。
42	本体	5.1.4	[項番] 9 [該当箇所] P31 5.1.4 (4)リスク保有 [意見内容] 更新漏れと思われる。 (4)リスク受容	御指摘を踏まえ、修正いたしました。

43	本体	5.1.5	[項番] 10 [該当箇所] P32 5.1.5 (1)(ア) さらに、対策を設計する際に、別紙2 に書かれている「対策項目で対応できるリスクシナリオ（例）」を参考にすることも有効である。 [意見内容] (1)前回1.1版のパブコメにおいて、別紙2の名称は、「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」に変更されたはずです。 (2) 本来は、そのコメントのように、「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。」のとおりに対応した上で公表してほしいと思います。 (3) (2)を実施することにより、本文記載の「参考することも有効」のようになるのではないかと考えます。 [理由] https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000256256 #15	ご指摘の(1)について、別紙2の名称は、「1.3. 本ガイドラインの構成」において、「「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」（以下、「別紙2」という。）」と記載させていただいております。 ご指摘の(2)(3)について、別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただきます。
44	本体	5.2.1	[項番] 11 [該当箇所] P41 5.2.1 (1) 手順1 医療情報の処理に関連し、どこにどのような機器や記憶媒体があるかを可能な限り明らかにする （図 5-) 。 [意見内容] 誤植 医療情報の処理に関連し、どこにどのような機器や記憶媒体があるかを可能な限り明らかにする （図 5-4) 。	e-govにて公開した案は正しい表記でしたが、総務省の報道発表にて公開した案に誤りがありました。
45	本体	5.2.1	[項番] 12 [該当箇所] P44 5.2.1 (1) 手順4 人が直接扱わない機器における情報の処理を「どこの」、「どの機器で」、「何が」、「どうされるか」の切り口で可能な限り明らかにする (図 5)。 [意見内容] 誤植 人が直接扱わない機器における情報の処理を「どこの」、「どの機器で」、「何が」、「どうされるか」の切り口で可能な限り明らかにする (図 5-7)。	e-govにて公開した案は正しい表記でしたが、総務省の報道発表にて公開した案に誤りがありました。
46	本体	5.2.1	[項番] 13 [該当箇所] P44 5.2.1 (2) 観点が異なるため、本節では、 2.2 で整理した医療情報システム等の代表的な提供形態として、アプリケーション、プラットフォーム、インフラそれぞれの提供における情報流の特定の観点について例示する 。 [意見内容] 2.2の記載が今回、変更され、アプリケーション、プラットフォーム、インフラの説明が削除されている。現状の2.2に合わせて、本節の説明の構成を修正すべきでと思われる。 または、5.2.1(2)の先頭にアプリケーション、プラットフォーム、インフラの説明を記載するのがいいのではないかと思われる。	御指摘を踏まえ、修正いたしました。
47	本体	用語集	[項番] 14 [該当箇所] P60 用語集 脆弱性 脅威によって悪用される可能性がある欠陥や仕様上の問題。 [意見内容] JISQ27000の用語の定義を採用すべきと思われる。 (変更案) 一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。 [理由] https://kikakurui.com/q/Q27000-2019-01.html	当該記載は、脆弱性について製造物の責任のみよって生じるものであることを意味しておらず、実際に意図しない欠陥や問題によって生じ得ることから、原案のとおりとさせていただきます。
48	本体	用語集	[項番] 15 [該当箇所] 用語集 [意見内容] 用語集にSDSの説明はあるが、MDSの説明がない。本文中にMDSも書かれているので、MDSの説明も書くべきと思われる。 用語： MDS(Manufacturer Disclosure Statement for Medical Information Security) 内容： 製造業者の医療情報システムを対象とした医療情報セキュリティ開示書の意味。 事業者が自ら提供するする医療情報システムのセキュリティ関連機能に関して、 標準化された書式で記載を行い、医療機関等から情報提供を要求されたとき情報提供 するためのもの。一般社団法人保健医療福祉情報システム工業会（ JAHIS ）及び 一般社団法人日本画像医療システム工業会（ JIRA ）により整備されている。	御指摘を踏まえ、修正いたしました。
49	本体	用語集	[項番] 16 [該当箇所] 用語集 [意見内容] 用語集のSDSの説明からシステムを削除すべきと思われます。 修正前：事業者が自ら提供する医療情報システム・サービスのセキュリティ関連機能に関して、 修正後：事業者が自ら提供する医療情報サービスのセキュリティ関連機能に関して、	御指摘を踏まえ、修正いたしました。
50	本体	参考文献	[項番] 17 [該当箇所] p.62（参考文献） [意見内容] ・「製造業者 サービス事業者 による医療情報セキュリティ開示書チェックリスト」 の年月が「2023年6月」と旧版の日付になっている。「2024年9月」に修正すべきと思われる。 [理由] 出典：JAHIS標準24-005 JAHIS「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.5.0 https://www.jahis.jp/standard/detail/id=1119	御指摘を踏まえ、修正いたしました。
51	SLA参考例	脚注1	[項番] 18 [該当箇所] パブコメ対象ではありませんが、更新すべきと思われる箇所を指摘いたします。 SLA参考例のP.2の脚注 [意見内容] https://www.jahis.jp/standard/detail/id=987となっているが、これは旧版Ver.4.1なので、最新版のVer.5.0ではhttps://www.jahis.jp/standard/detail/id=1119	御指摘を踏まえ、修正いたしました。

52	SLA参考例	脚注5	[項番] 19 [該当箇所] パブコメ対象ではありませんが、更新すべきと思われる箇所を指摘いたします。 SLA参考例のP.80の脚注 [意見内容] 「「JAHIS 参照」とは、当該項目について「JAHIS リモートサービス セキュリティガイドラインVer.3.1a」（一般社団法人 保健医療福祉情報システム工業会 医療システム部会 セキュリティ委員会 JAHIS/JIRA 合同リモートサービスセキュリティ作成WG）に付属する「リモート保守サービスSLA サンプル（見本）」、及び「リモート保守サービスSLA サンプル解説付き（テンプレート）」の内容を参照して、検討することが望ましい旨を示す。」とあるが、RSSガイドラインの最新版はVer.4.0	御指摘を踏まえ、修正いたしました。
53	本体	3.1.2	# 3.1.2.「直接契約の対象となっていない事項」について 弊社はクラウド型サービスを提供しておりますが、ここの「直接契約の対象となっていない事項」について記述は （たとえばオンプレミス型サービスとあわせて）コンサルティングを提供している事業者向けに記載されていると感じました。 例として医療情報が投稿されるチャットやストレージを提供している事業者においても、直接契約の対象となっていない 事項、たとえばそのサービスに情報を保存する医療機器などに関する情報を提供するかというと、考えにくいと感じます。 クラウド型サービスにおいてはどの程度ここの記載が適用されるのか、明確にしていただきたいです。	当該記載は、コンサルティングを提供している事業者のみならず、システムの導入等を行うベンダー等が、医療機関に対して、医療機関等が医療情報システム等に用いる機器に関するセキュリティ情報も含めて情報提供すべきであるということを意図したものであり、原案のとおりとさせていただきます。
54	本体	3.2.1	# 3.2.1.「望ましい」表記の扱いについて こちらで記載されている内容は事業者の判断や活動を支援するガイドラインではなく、筆者の感想となっています。 「合意の内容に医療情報システム等の機能や性能、仕様などに加えて、情報提供範囲や非常時における 対応などについても明示的に示すこと」「医療機関等と事業者が限行に際して遵守すべき範囲を契約内容に 明示すること。」など記載いただきたいです。	本ガイドラインは、リスクベースアプローチの考え方を採用しており、義務としない事項については「望ましい」と記載しているため、原案のとおりとさせていただきます。
55	本体	4.4	# 4.4で「特に、プライバシーマーク認定を取得していることが望ましい」としている件 2.0版からISMS認証と比較して「特に、プライバシーマーク認定を取得していることが望ましい」としている点について、 次に述べる観点からプライバシーマークがISMS認証に対する優位性を持つとは考えにくいです: - 取得やその維持に実効的な意味が薄い点。2007年の大日本印刷の事例が象徴的だが、その後の改善も見られない（文書「PMK500」を参照） - 全社に一括で適用されるため、効率的でない運用を作り込む可能性が高く、運用コストが合理的でない 一方でISMSは国際認証としての信用と運用を持ち、プライバシーマーク認定よりも柔軟かつ実践的です。 もし個人情報に特化した認証であることを評価されているのであれば、ISO27018などの他の個人情報管理に 関する認証も併記することをご検討いただければと思います。	参考意見とさせていただきます。ISO27018等の記載も含め、本ガイドラインにおける第三者認証等の取得に関する記載については、今後の検討とさせていただきます。
56	本体	5.1.6	# "5.1.6 リスクコミュニケーション" の表現を明確にしていただきたい 「医療機関等側から説明を求められた場合の対応の表示」とありますが、様々な解釈が可能な表現であり 判断の頼りにするガイドラインとして不適当ではないかと考えます。具体的には以下のような解釈が可能です: - 医療機関様から事業者に説明を求めた場合にどう対応するか、その窓口・営業日・対応範囲を契約内容に記載。 たとえば「問い合わせ用フォームを使って質問をした場合に3営業日で回答します」など。 - 医療機関様から事業者に要求できる説明事項を種類分けし、それぞれに対して行う対応を契約内容に記載。 たとえば「外部連携機器の追加について、期日の半年前にはご連絡ください」など。 表現を見直すとともに具体例を追加することで、解釈の余地を小さくしていただきたいです。	本ガイドラインは、リスクベースアプローチの考え方を採用しており、リスクコミュニケーションの具体的な方法について示すものではありませんので、原案のとおりとさせていただきます。
57	本体	6.5	6.5. 外部保存の要求事項" が参照する文書を明確にしていただきたい 6.5.で外部保存改正通知「第2診療録等の外部保存を行う際の基準」「1電子媒体により外部保存を行う場合」が 参照されていますが、具体的にどの文書なのか判別ができませんでした。版なら広く配布元URLの提示をお願いいたします。	外部保存改正通知については、以下のURLをご参照ください。 https://www.mhlw.go.jp/file/06-Seisakujouhou-10800000-Iseikyoku/0000118707.pdf なお、本ガイドラインに記載している他のガイドラインや通知と同様、本ガイドラインへのURL等の記載は行わず、原案のとおりとさせていただきます。
58	本体	4.4	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を参考 医療情報を扱う対象事業者及び、直接取り扱わない対象事業者にプライバシーマーク認定またはISMS認証の取得を法律で義務化してもいいと思います。 大半の日本国民は情報漏洩が起きても訴訟しない(出来ない)人ばかりだと思いますので厳しい基準を設けるべきです。	参考意見とさせていただきます。
59	本体	4.1	（１）意見１ Ａ文書頁／章番号：２５（２１）／４．１ Ｂ該当箇所：表４－１ 医療機関等へ情報提供すべき項目 Ｃ意見内容：医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目と記載されておりますが、「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」では、「外部保存を受託する事業者の選定基準」が外部保存に限定されない形で示されている。「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」に合わせた形で文言を修正して頂きたい。 （修正案） ５．医療情報システム・サービス事業者との協働における事業者選定の遵守事項に従い、少なくとも確認する必要がある項目	御指摘を踏まえ、表4-1「目的」欄の記載を、「事業者の選定基準として少なくとも確認する必要がある項目」に修正いたしました。
60	本体	4.1,4.4	（２）意見２ Ａ文書頁／章番号：２５（２１）と２７（２３）／４．１と４．４ Ｂ該当箇所：表4－１ 医療機関等へ情報提供すべき項目４．４本文 Ｃ意見内容：４．４では最低限の適格性の提示のために、第三者認証として「プライバシーマーク認証又はISMS認証を取得することとしているが、表４－１では「医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目」の情報提供すべき項目として、「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「プライバシーマーク認定、ISMS認証のいずれも取得していない場合は、？」が並列に記載されており、プライバシーマーク認定又はISMS認証を取得しなくとも適格性を医療機関に示すことができるように読める。不整合が起こっているため整合性をとった形で記載して頂きたい。	「プライバシーマーク認定、ISMS認証のいずれも取得していない場合は、「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「クラウドセキュリティ認証等」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又は医療情報システム等の適切な運用管理能力の有無を確認すること」については、プライバシーマーク認定、ISMS認定のいずれも取得していない場合の対策をお示ししているものであり、プライバシーマーク認定、ISMS認証のいずれも取得しなくても医療機関等へ適格性を示すことができることを意図した記載ではありません。
61	本体	4.1	（３）意見３ Ａ文書頁／章番号：２５（２１）／４．１ Ｂ該当箇所：表４？１医療機関等へ情報提供すべき項目 Ｃ意見内容：表４－１では「医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目」の情報提供すべき項目として、「民間事業者による医療情報に係るクラウドサービスの評価」（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）が示されているが、これは脚注に記述があるように、同表の「医療情報システム等の安全管理に係る評価（４．３参照）」に関わる第三者評価であるので、同表の「医療情報システム等の安全管 理に係る評価（４．３ 参照）」の「情報提供すべき項目欄」に「医療情報システム等の安全管理に係る評価の 結果。内部の独立した監査部門や第三者機関（例えば「民間事業者による医療情報に係るクラウドサービスの評価」（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）の評価結果が望ましい」と記載位置を修正してはどうか。	既に同様の内容としては4.3に記載していますので、原案のとおりとさせていただきます。
62	本体	5.1.4	（４）意見４ Ａ文書頁／章番号：３４（３０）／５．１．４ Ｂ該当箇所：図5-2影響度と顕在化率に応じた選択肢の考え方 Ｃ意見内容：本文は「リスク共有」であるが、図中では「リスク移転」となっている。本文中の文言と平仄を取るため修正をされたい。	御指摘を踏まえ、修正いたしました。
63	本体	5.1.5	（５）意見５ Ａ文書頁／章番号：３６（３２）／５．１．５（１）（イ）マル３ Ｂ該当箇所：マル３ネットワーク経路における考慮事項 Ｃ意見内容：マル３本文中に「セキュアなネットワーク」と記載があるが、医療情報システムの安全管理に関するガイドラインに記載されている事項を補足することで、読者との認識のずれを防ぐためQAにて、「セキュアなネットワーク」を補足してはどうか。 さらに、本文中に「特にオープンなネットワークにおける接続に際して HTTPS 利用における TLS を用いた暗号化等 が例示されている。そこでは、HTTPS 接続においては、」は削除して「HTTPS 接続を用いる場合、」を追加してはどうか。 理由として、この文書があると医療情報安全管理ガイドラインではセキュアなネットとしてTLSを最もセキュアなものとして推奨しているように誤解される為、それぞれの方式に対して併記する形式を提案している。	御指摘を踏まえ、「セキュアなネットワーク」について脚注に追記いたしました。また、医療情報安全管理ガイドラインが、セキュアなネットとしてTLSを最もセキュアなものとして推奨しているものではないと思料しますが、TLSが例示の一つであることが明確になるように、「HTTPS接続を利用する場合は」の文言を追記いたしました。
64	全体	全体	全体の構成上、医療機関等と事業者側がそれぞれにおいてリスクアセスメントを実施し、リスク対策、対応を検討し、行動を起こす内容となっているが、医療機関等や事業者の自助努力（対応が難しい点については合理的説明を求める等含む）のみではなく、それぞれの規模、実務体系に配慮した指針でなければ、形骸化し、本来取るべき対応内容が低下する恐れがあると考える。 ガイドライン本来の在り方として、医療機関等や事業者の規模、実務等に配慮した対応指針のご検討をいただきたい。	参考意見として承りました。本ガイドラインのあり方につきましては、今後の検討とさせていただきます。
65	本体	5.1.6	「経産省・総務省ガイドライン第2.0版パブコメ_ガイドライン案.pdf」P37 【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】とあるが、コラムの事例が古い。記載事例以降の被害事実は発生しているため、ガイドラインの改定に合わせ、最新の事例を紹介すべき。	原案における事例は、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ことを顕著に表している例であるため、原案のとおりとさせていただきます。
66	SLA参考例	2.(3)⑦	「経産省・総務省ガイドライン第2.0版パブコメ_サービス仕様適合開示書_SLA参考例.pdf」P34 7 監査項目内の備考 「・クラウドサービスの特殊性から、報告方法については、本SLA 参考例６． ５(1)2にしたがって実施することを想定し、？以下、略」とあるが、「本SLA 参考例６． ５(1)2」とは、以下、2つの表中の年次報告事項を意味しているか。 ２． ２ サービスごとの各項目へのSLA 項目の適用 (1) 相対契約によるサービス (2) 約款契約によるサービス	ご認識のとおりの内容を意味しています。
67	SLA参考例	2.(4)③	「経産省・総務省ガイドライン第2.0版パブコメ_サービス仕様適合開示書_SLA参考例.pdf」P39 再委託先・連携事業者の詳細 従来は「データセンターについては、明示の対象は事業者までとし、セキュリティ上の対応としてデータセンターの所在地等までは明示しないのが一般的であると考えられる。」との記載があったが削除されたのはなぜか。最近のサイバー攻撃等を考慮し、「データセンターについては、明示の対象は事業者までとし、セキュリティ上の対応としてデータセンターの所在地等までは明示しないことが望ましい」ということを備考へ明記するのがよい。	御指摘を踏まえ、データセンター等、医療情報を保存する情報機器が設置されている場所の開示水準ついて、追記いたしました。

68	SLA参考例	2.(6)①	「経産省・総務省ガイドライン第2.0版パブコメ_サービス仕様適合開示書_SLA参考例.pdf」P49 (6) 運用内容 1 運用組織・規程等（ｊ）運用に関する規程　解説 2.(1).1「本サービスの目的と概要」の備考に、「クラウドサービスのように、複数の顧客に対して同じSLA で対応する場合には、個々の顧客の特定を想定した記載ではなく、一般的なサービスにより実現することなどが目的とされる。」とあるように、事業者側が作成する運用管理規程も提供するサービス形態により異なる。 そのため、本項目の備考に以下を記載してはどうか。 「クラウドサービスのように、複数の顧客に対して事業者において同じ運用管理規程である場合は、個々の顧客の特定を想定した記載ではないため、事業者が作成する運用管理規程を参考に医療機関等の運用管理規程への条項採否を調整する。」	医療機関等における運用管理規定は、医療機関等が主体的に検討することが望ましいと思料しますので、原案のとおりとさせていただきます。
69	本体	表4-1	（項番１） （該当箇所） 別紙2　提供事業者における安全管理ガイドライン第 2.0 版（案）P22 表4-1 （意見内容） 「民間事業者による医療情報に係るクラウドサービスの評価」（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）」を「プライバシーマーク認定、ISMS 認証のいず れも取得していない場合」の認証等が確認できない場合の監査資格者に加えて頂いていますが、次の項番２に示す理由で、表4-1の「医療情報システム等の安全管理に係る評価（4.3 参照）の「情報提供すべき項目欄」に移動していただきたい。それにより4.3と整合性が取れます。 (理由) 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の評価は、本文4.3「医療情報システム等の安全管理に係る評価」に記述された第三者評価機関として脚注21に記述されていて、プライバシーマーク以下で例示された管理能力の評価である「対象事業者の適格性を評価する第三者認証」とは異なっています。なお、脚注21の、「医療情報に関する IT サービスに関するガイドラインへの適合性評価」は表4-1に追加頂いた「民間事業者による医療情報に係るクラウドサービスの評価」が正しいです。	原案にて、既に表4-1の「情報提供すべき項目欄」に「民間事業者による医療情報に係るクラウドサービスの評価」を記載しております。脚注21については、御指摘を踏まえ、修正いたしました。
70	本体	表4-1	（項番２） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）Ｐ２２　表4.1 「医療情報システム等の安全管理に係る評価（4.3 参照）欄」の「情報提供すべき項目」欄 （意見内容） 以下の内容とする。 「医療情報システム等の安全管理に係る評価の結果。対象事業者内部の独立した監査部 門や第三者機関（例えば、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 マーク適合性評価））が望ましい。」 （理由） ４．３の主旨を生かし、担当者自らのみの評価による開示で終わってしまうことをへらし、開示内容の信頼性及び客観性を上げ、世の中の医療情報システムの全体の安全性を高める為。。	既に同様の内容としては4.3に記載していますので、原案のとおりとさせていただきます。
71	本体	4.3	（項番３） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）4.3 最後の行へ追加。脚注２１から本文への移動 （意見内容） 脚注２１を本文として以下の記述を最後に追加する。 「第三者機関による評価として、例えば、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）による、「民間事業者による医療情報に係るクラウドサービスの評価」があげられる。」 「脚注２１」として、4.3の補足の意味で安全管理の評価レベルの以下の説明を追加する 「医療情報システム等の安全管理に係る評価としては、１）安全管理の項目の自己点検シートを開示する方法　２）HISPROマーク適合性評価のように、開示された内容を設計書、運用管理規程や重要事項説明書等のエビデンス資料を確認し適合性を評価する方法　３）システムの求める安全管理目標に対する評価保証レベルに合わせて動作確認を行うISO/IEC15408に基づくITセキュリティ評価及び認証制度があり、医療情報システムの安全管理の評価保証レベルと評価費用、評価期間が変わってくる。」 （理由） 開示の段階で終わってしまうと、ガイドライン等を提供事業者に理解不足で開示や、医療機関等が開示内容を十分理解できない開示となっていることが有る。脚注21を本文として記述を追加することによりHISPROマーク適合性評価の有効性の理解がすすみ、少なくともガイドラインの理解不足が減り、結果として、システムの安全管理が高まることになる。 併せて、新たな脚注21として追加を提案した主旨は、安全管理の保証レベルの概念を理解して頂くものです。ガイドライン等への準拠性の評価として「自己評価による開示」、「開示内容に対する第三者による エビデンス評価」、さらに「システムの動作評価」のレベルがあることの理解が重要である。。 また、これにより、4.4の提供事業者の適格性（安全管理に関するマネージメント能力等）を全体的に評価するものとは異なっていることの理解が深まることが期待できる。	既に同様の内容としては4.3に記載していますので、原案のとおりとさせていただきます。また、脚注21の記載について、4.3及び当該脚注は、医療情報システム等の安全管理に係る評価において第三者による評価を受けるべきであることを趣旨としたものですので、ご意見の「自己評価による開示」、「システムの動作評価」の記載については今後の検討とさせていただきます。
72	本体	4.4	（項番４） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）P23 4.4 ４行目 （意見内容） 「また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。」 を以下に修正する。 「また ISMS 認証や表4-1で示す他の認証については、対象事業者の情報システム管理が適正になされていることを認証するものであり、個々の提供システムの安全管理対策の有効性までを認証するものではないことに留意する必要がある。」 また、 「そのため、ISMS 認証のみを取得する場合には、事業者における具 体的な管理方法の説明等を検討する等、医療機関等から有効性を示す資料の提供を求めら れた場合に対応できる状態としておくことが望ましい。」 を以下に修正する。 「そのため、ISMS 認証等のみを取得する場合には、事業者における具体的な提供システムに関連した医療情報システムに要求される管理方法の評価を含める等、医療機関等からその有効性を示す資料の提供を求めら れた場合に対応できる状態としておくことが望ましい。」 また、4.4ではPマークかISMSが必須になっているのに、表4.1では他の評価も認めているので整合性を図る表現として頂きたい （理由） 4.4と表4-1の整合性を図るため。また、ISMS認証等が医療機関へ提供するシステムや医療ン情報システムに関連した評価を対象事業者全体の包括的な評価で認証を受けている場合に対する注意として補足した。	4.4のご意見をいただいている記載については、ISMS認証を取得する場合の留意点について明記しているものであるため、原案のとおりとさせていただきます。
73	本体	5.1.5	（項番５） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第2.0版（案）P32(3)ネットワーク経路における考慮事項 （意見内容） 「対象事業者は、提供するサービスに応じ、原則としてセキュアなネットワークを採用し、ネットワーク経路を適切に選択することが必要である。」 の後に 「医療情報安全管理ガイドラインでは、接続先が限定されている、あるいは接続先までの経路等が管理されているオープンではないネ ットワークを「セキュアなネットワーク」と称することとしている。 （理由） セキュアなネットワークの用語が突然出てくるの補足した方がわかりやすい。 セキュアなネットワークは医療情報安全管理ガイドラインで定義しているので、 セキュアネットワークの詳細な説明は医療情報安全管理ガイドラインを引用して Q&Aに追加していただきたい。	御指摘を踏まえ、「セキュアなネットワーク」について脚注に追記いたしました。
74	本体	5.1.5	（項番６） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）P33の２行目 （意見内容） 「特にオープンなネットワークにおける 接続に際してHTTPS 利用におけるTLSを用いた暗号化等が例示されている。そこでは」を削除する。 また、４行目 「HTTPS 接続においては」の後に「クライアント認証を用い」を いれ、「TLSの設定はサーバ/クライアントともに CRYPTREC が定める---」と続ける。 （理由） 原文の記述がありと医療情報安全管理ガイドラインがTLSを推奨しているように読め、他のネットワークも推奨していることが読み取れなくなる。 各セキュアなネットワークの暗号化方式を並列した位置づけで説明すべきである。	医療情報安全管理ガイドラインが、セキュアなネットとしてTLSを最もセキュアなものとして推奨しているものではないと思料しますが、TLSが例示の一つであることが明確になるように、「HTTPS接続を利用する場合は」の文言を追記いたしました。
75	本体	図5-2	（項番７） （該当箇所） 別紙２　安全管理ガイドライン第 2.0 版（案）P30　図5-2 ＜意見内容＞ 図中の「リスク移転」は「リスク共有」に修正すべき。。 ＜理由＞ 本文中でもP31で（３）リスク共有となっている。	御指摘を踏まえ、修正いたしました。
76	本体	2.1	1.「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、「しかし、医療情報システム等の売買契約等のみであり、運用又は管理、保守に関する契約等がない場合は、「契約等」に含まれない。」と記載されている。売買契約等の場合に除外することは明確に記載されている。しかし、売買して、いわゆる保守契約の場合に除外するようには読めない。有識者委員会でも、「保守については、保守と運用を含む表現を検討する」とされていた。売買契約しても、最低限のハードウエア故障時の対応等の保守契約が含まれる場合がある。あくまで、いわゆる「サービス」のみが含まれ、その「サービス」では、外部保存以外のサービスも含むような記載が望まれる。(修文案) しかし、医療情報システム等の売買契約等のみであり、サービス(運用又は管理及びそれらに関する保守)に関する契約等がない場合は、「契約等」に含まれない。」	一般論としての対象範囲の考え方については、FAQに今回追記させていただいております。ご意見の売買契約と保守契約の考え方については、個別サービスの事情によって判断が異なることから、本体及びFAQへのこれ以上の追記は行わず、原案のとおりとさせていただきます。
77	本体	図2-2	2. 図2-2の対象事業者として「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」と記載されている。2.1の記載とも平仄が図られていない。(修文案) 「医療機関等とのサービスに関する契約等に基づいて医療情報システムを用いたサービス・システムを提供する事業者」	図2-2の記載は、本文の2.1①の記載に合わせておりますので、原案のとおりとさせていただきます。
78	本体	2.1	3.「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、「本ガイドラインが対象とする事業者は、(まる１) 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、(まる2)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、(まる3)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 （以下、これらを総称して「対象事業者」という）である。」と記載されている。しかし、必要以上に範囲が広く誤解される可能性がある。過去の有識者委員会の対応等に合わせて、適切な記載に修正すべきではないか。(修文案) 「本ガイドラインが対象とする事業者は、(まる１) 医療機関等とのサービスに関する契約等 に基づいて 医療情報システムを用いたサービス・システムを提供する事業者 、(まる2)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を用いたサービスに必要な資源や役務を提供する事業者、(まる3)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医療情報システムを用いたサービスを提供する事業者 は （以下、これらを総称して「対象事業者」という）である。」	参考意見として承りました。本ガイドラインの対象事業者については、今後の検討とさせていただきます。
79	本体	表4-1	4.「表 4 -1 医療機関等へ情報提供すべき項目」において、特に「医療機関等との共通理解を形成するために情報提供すべき項目」の「運用管理規程に含める事項」等は、医療情報システムを用いたサービスを提供するための運用又は管理に、事業者側で考慮すべき項目であり、システム提供をする事業者には適切ではなく過剰に思えます。表 4 - 1 のタイトルを「サービス提供事業者(対象事業者)が医療機関等へ情報提供すべき項目」と明記すべきでは。 これにより、脚注19の表記とも平仄が図れる。	参考意見として承りました。表4-1における情報提供の主体を明記すべきかについては、今後の検討とさせていただきます。
80	本体	用語集	5. 用語集のＳＬＡでは、「書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した 、サービス提供者と顧客との間の合意文書」とあるため、医療機器等の販売でかつ、保守、定期点検等の契約のみでは、サービスの提供がないため、SLAが要求されないと思われるが、この理解で正しいか？	医療機器等の販売のみでは対象外となりますが、保守、定期点検に係る契約については対象となります。

81	本体	3.2.1	6.「3.2.1契約前の合意形成及び契約中の合意の維持」において「対象事業者は、医療機関等との共通理解の上で、契約書やSLA等の契約上の文書を作成し、医療機関等と明示的な合意を形成すること。」と記載されている。非常に重要な点だと思いますが、ＳＬＡとか契約とかが必須なのではなく、明文化及びそれに基づく合意がより重要で強調すべきではないかと考えます。(修文案)「対象事業者は、医療機関等との共通理解に基づき、契約書や必要に応じてSLA等の契約関連文書を作成し、医療機関等と明示的な文書による合意を形成すること。	原案においても、いただいたご意見と趣旨は相違ないことから、原案のとおりとさせていただきます。
82	本体	3.2.1	＜意見No.1＞ 【該当箇所】 ガイドライン第2.0版（案）「3.2.1 契約前の合意形成及び契約中の合意の維持」等口 【意見】 近年における医療情報システムに対するサイバー攻撃の多様化・巧妙化によるセキュリティ対策の変化を踏まえたものとなっており、本ガイドライン案の改正内容についてはおおむね賛同いたします。一方で、本ガイドラインについて事業者と同様、医療機関側等への周知・浸透を関係省庁と連携しながら推進していただくことを要望いたします。口 【理由】 本ガイドライン（案）では、医療機関等と事業者の間において共通理解を得て取り決めを行うこととされている項目をはじめ、事業者から医療機関等側の協力を求めることが必要な場合が散見され、医療機関側の対応方針等によっては両者間の調整が困難になることも見込まれ、事業者の過度な負担になる可能性があるため。	参考意見として承りました。本ガイドラインの周知につきましては、今後の検討とさせていただきます。
83	本体	2.1	＜意見No.2＞ 【該当箇所】 ガイドライン第2.0版（案）「2.1 本ガイドラインが対象とする医療情報と事業者」口 【意見】 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 第6.0版」（以下「厚労省ガイドライン」という。）における医療機関等の特性に応じた参照パターンと同様の整理をすることで、本ガイドライン案における各項目の適用場面を明確にすることが望ましいと考えます。口 【理由】 先に策定されている厚労省ガイドラインは医療機関等の特性に応じた本ガイドラインの参照パターンとして「オンプレ型」及び「クラウド型」の区分を設け、項目ごとの適用関係が整理がなされています。一方で、本ガイドライン案は同様の参照パターンで整理がされておらず、規定項目ごとの適用場面が不明瞭な場合が散見されるため（例：「 5.1.5 リスク対応策の設計・評価」-（イ）-「3. ネットワーク経路における考慮事項」に規定されているHTTPS 利用におけるTLSを用いた暗号化等の手法は、オンプレ型又はクラウド型のいずれに適用されるか等）。	本ガイドラインは、リスクベースアプローチの考え方を採用しており、適用場面を明確に区分することは、適用場面に限られた対策のみが求められるという誤解、ひいては、本ガイドラインの実効性の低下につながる懸念がありますので、原案のとおりとさせていただきます。
84	本体	表4-1	＜意見No.3＞ 【該当箇所】 ガイドライン第2.0版(案)「4.1 医療機関等へ情報提供すべき項目」「情報提供すべき項目」第6項目（「財務諸表等に基づく経営の健全性」）口 【意見】 財務諸表等の開示に関しては任意としてはどうか。（※今回の改正箇所ではないが、現状を踏まえて意見提出させていただくもの。） 【理由】 主にスタートアップは「J カーブ」と呼ばれる成長曲線に特徴があり、形式的な財務状況のみでは必ずしも実態をよく表現しきれず、誤った判断を誘導する可能性があるため。また財務諸表は多くの未上場企業において広くは明らかにしていない機密事項であるが、サービス提供に伴い不特定多数人の目に触れる形で実質的に公開されることになり、情報管理上リスクに曝されるため。	参考意見として承りました。財務諸表等の開示等、サービス継続が可能であることの担保のあり方については、今後の検討とさせていただきます。
85	本体	表4-1	＜意見No.4＞ 【該当箇所】 ガイドライン第2.0版(案)「4.1 医療機関等へ情報提供すべき項目」「情報提供すべき項目」第6項目（「財務諸表等に基づく経営の健全性」） 【意見】 財務諸表等の「等」には何が含まれるかを具体的に例示されたい。特に、医療機関及び事業者の双方にとってより簡便かつ合理的な確認手段があるのであれば明記されたい。（※今回の改正箇所ではないが、現状を踏まえて意見提出させていただくもの。） 【理由】 財務諸表から経営の健全性を判断するには相応の専門知識が求められるため医療機関の規模・属性に応じてより効果的な確認手段の選択肢が示されることが望ましいため。また財務諸表そのものの事実上の公開を避けたい未上場企業に対して規制対応上の現実的な選択肢が与えられることが望ましいため。	「等」については、キャッシュフロー等の、事業者がサービス継続が可能であることを担保できる資料を想定していることから、原案のとおりとさせていただきます。
86	FAQ	1.4	・意見内容 具体的なユースケースとして、以下の場合は、当ガイドラインの対象となりますでしょうか？ （１）医療機関等が患者等に渡した医療情報を、患者等が手入力するPHRサービス （２）医療機関等が患者等に渡したQRコード自体に（閲覧用のURLではなく）PHR情報そのものが格納されており（お薬手帳QRコードと同様のあり方）、PHRサービスにて当該QRコードを読み込む形でPHRを取り込むPHRサービス （３）本ガイドラインの対象となるPHRサービスとデータ連携（API連携）するPHRサービス （４）マイナポータルAPI経由で、医療機関由来の３文書６情報・電子処方箋等を取得するPHRサービス なお、いずれもあくまで患者等にPHRが渡ったあとのPHRの自己管理用途であるため、本ガイドラインの対象外とすべきと考えています。 特に（３）が本ガイドラインの対象となると、今後のデータ連携の時代において、あらゆるPHRサービスが本ガイドラインの対象となる懸念があります。 背景として以下のような研究も進捗しており、PHRサービス間のデータ連携が今後発展することが期待されている認識です。 https://www.amed.go.jp/program/list/14/05/015.html	本ガイドラインが対象とする事業者への該当性については、個別サービスの対象範囲の判断は行っておらず、以下条件に照らして、自らご判断いただくことになります。 ①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、 ②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 ③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
87	本体	脚注5	（項番１） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）　P1　脚注5 （意見内容） 可用性の説明が抜けています。 （理由） 記入漏れと思われる為	e-govにて公開した案は３要素の説明をいずれもP1に記載しておりましたが、総務省の報道発表にて公開した案では可用性の説明のみP2に記載されており、見えづらくなっておりました。
88	本体	1.1.5	（項番２） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案）　P4 「1.1.5 状況の変化に対する改定の必要性」の最後 （意見内容） 以下を補足として追加願いたい。 「別紙 2 は、医療情報システム等の運用が適切であるか、リスクマネジメントを 通じて、最低限確認するためのものと位置づけ、改定せず、そのまま利用する。」 （理由） 別紙2の扱いはFAQにも触れられているが本文でも明確にする為	別紙2の位置づけや使用法については、「1.3.本ガイドラインの構成」及び「5.1.5.リスク対応策の設計・評価」に記載していること、別紙２の最新版ガイドラインへの対応は、今後の検討とさせていただくことから、原案のとおりとさせていただきます。
89	本体	3.1.1	（項番3） （該当箇所） 別紙２　提供事業者における安全管理ガイドライン第 2.0 版（案） P13 下から３行目 （意見内容） 「また、医療機関等は、本ガイドラインに従ってクラウドサービス提供事業者を 適切に監督する必要があり、」 を以下に修正 「また、クラウドサービス提供事業者も医療機関等より適切に監督を受ける必要があり、」 に修正。 （理由） 本ガイドラインは対象事業者を主語にしたガイドラインであるため。	ご認識のとおり、本ガイドラインの主体は対象事業者でありますが、当該記載での監督の主体は医療機関等である旨をわかりやすくするための記載であるため、原案のとおりとさせていただきます。
90	SLA参考例	4.2	（項番4） （該当箇所） 別添２-２　サービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例 P4　4.2 下から3行目 （意見内容） 「このような合意を外部の事業者に対して委託を行う必要がある。」 を以下に修正する。 「このような合意を外部の事業者に対して委託を行う必要がある場合がある。」 （理由） 原文ですと意味が良く取れない為。	御指摘を踏まえ、修正いたしました。
91	SLA参考例	図1	（項番5） （該当箇所） 別添２-２　サービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例 P7 図１ 真ん中の赤ボックス内 （意見内容） 「MDS/SDS又は要求仕様適合開示書の作成」を「サービス仕様適合開示書又はMDS/SDSの作成」とする。 （理由） 「サービス仕様」とすべきところが「要求仕様」となっています。 記述確認漏れと思われます。	御指摘を踏まえ、修正いたしました。（御指摘は、図2であると思料いたします。）
92	SLA参考例	図2	（項番6） （該当箇所） 別添２-２　サービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例 P8 図2 （意見内容） KPIの説明を図中に追加して頂きたい。 （理由） KPIに不慣れな読者もいると思われる為	御指摘を踏まえ、追記いたしました。