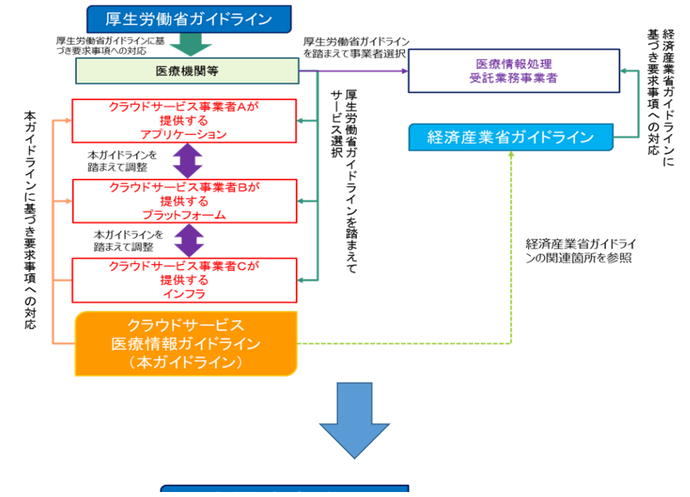
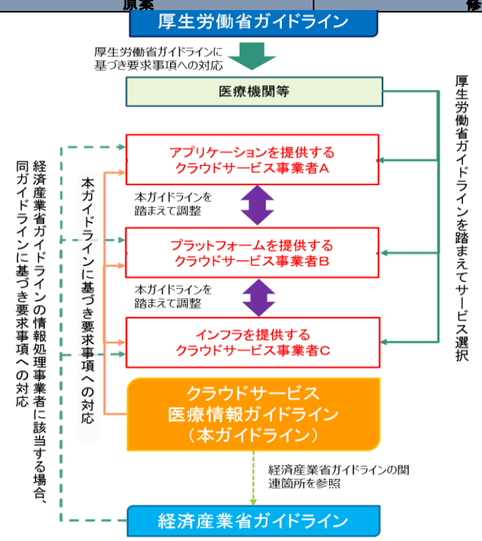
別紙2

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
1	個人A	個人	GL	全般	全般	情報の完全性が脅かされた場合、具体的に例示するならばアレルギー情報を紛失や攻撃者に削除された場合、患者はアレルギーのある医薬品を処方されたことによるアナフィラキシー反応により生命を脅かされる可能性がある。 よって医療情報に関しては情報の完全性も十分に担保されなければならない点に注意されたい。 本ガイドラインには「医療情報の完全性」が上記に示すように重要である事の指摘と具体的対策が不足していると感じた。	医療情報の完全性の重要性については十分に認識しており、第3章において必要な要求事項を設けておりますが、その重要性をより明らかにするため、ご指摘を踏まえて1.1.1に追記いたします。	1.1.1 「・・・高い保護方策が求められる。」	1.1.1 「・・・高い保護方策が求められる。また、医療従事者が利用する医療情報の完全性が損なわれると、適切な医療行為が行われない危険性がある。」
2	HEASNET	法人	GL	全般	全般	要求事項のうち、本来であればe-文書法の対象となる記録に対して適用されるものが、e-文書法の対象外の記録にも適用されているものが複数ある。e-文書法の対象でなく真正性、見読性、保存性を求められていない記録であっても、e-文書法の対象と同様に措置する必要があるか。 例として、"3．2．8災害等の非常時の対応についての安全管理対策（2）（ア）障害時における見読性確保に関する安全管理対策"は、e-文書法で求められる見読性に対する内容であり、全てのサービス内容において、過剰な対策を行いコストが必要となることにならないか？	ご指摘のとおり、厚生労働省ガイドラインでは、第6章で医療情報の取扱い全般に関する安全管理対策を示すとともに、第7章で保存義務のある診療録等を電子的に保存する場合の安全管理対策、第8章で保存義務のある診療録等を医療機関等の外部に保存する場合の安全管理対策、第9章でe-文書法に基づいてスキャナ等により電子化して保存する場合の安全管理対策を付加的に示しています。 その一方で、厚生労働省ガイドラインでは、保存義務がない文書等であっても、個人情報の保護について留意しなければならない文書等について、バックアップ情報等を含めて、それらを破棄せず保存している限り、7 章及び 9 章に準じて取り扱う必要があるとしています。また、法定保存年限を超過する等により、保存義務がなくなった診療録等を外部保存する場合も、8章に準じて取り扱う必要があるとしています。 このように、厚生労働省ガイドラインでは、法定保存義務がなくても、法定保存義務のある医療情報と同等の真正性・見読性等を確保することが求められていることを踏まえ、本ガイドラインでは、その趣旨がより明確になるよう、「3．2 医療情報サービスに求められる安全管理に関する要求事項」において、全ての医療情報に求められる安全管理対策を掲載しつつ、その中で特に法定保存義務がある医療情報に求められる安全管理対策についてはその旨記載するとともに、「3．3 外部保存に関する要求事項」において、法定保存義務のある医療情報に求める安全管理対策の記載場所を一覧にして記載する形としております。 上記のとおり、原案において、法定保存義務に応じて安全管理対策を示しておりますので、ご懸念は当たらないものと認識しています。		
3	HEASNET	法人	GL	全般	全般	クラウドサービス事業者に対する要求事項の記載が、医療機関等がクラウドサービス事業者に求めるべき事項になっている項目が多いため、クラウドサービス事業者が守るべき要求事項として整理していただきたい。 例： p.77 クラウドサービス事業者が無線LANを提供することは考えにくい。	全般的に再度確認し、修正が必要なものについて修正しております。 なお、ご指摘で例示いただいた要求事項については、医療機関等が自らの無線LANを用いようとする場合について、クラウドサービス事業者に対し、医療機関等との責任分界等を定めるよう求めるものでありますので、原案のとおりとさせていただきます。		
4	アマゾンウェブサービスジャパン株式会社	法人	GL	全般	全般	I. 全体について 1．本ガイドラインが、医療情報の取扱いにおいてクラウドサービスの利用が普及しつつある状況を踏まえたうえで、従来のASP/SaaS中心のガイドラインから、PaaS、IaaS等に対象を広げ、また、サービスの多様化を考慮して記載内容も広げられたことについては支持します。 しかしながら、本ガイドラインは、IaaS、PaaS、SaaS等の種類又はプライベートクラウド、パブリッククラウド若しくはそのハイブリッドという形態が異なる多様なクラウドサービスについて、「クラウドサービス」とひとくくりにまとめて詳細な記述をしていることから、どのようなクラウドの種類やサービスの特徴がある場合に当該記載が該当するのかということが不明であり、クラウドサービスの利用者に誤解を招く可能性があるため、その観点から本ガイドラインの記述を整理すべきであると考えます。 そこで、まず、第1章において、「クラウドサービス」に関し、明示的にプライベートクラウド、パブリッククラウド、IaaS、PaaS、SaaSについての記載を追記するよう求めます。これにより、「クラウドサービス」が、実際は、多様なクラウドサービスを意味していることが利用者に明確に伝わるようになると考えます。	ご指摘の観点については、まず、1.2.2において、「ASP・SaaS」、「PaaS」、「IaaS」を定義し、それぞれクラウドサービスの一つであることを明記しております。また、1.1.1(5)において「今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている」ことを記載しております。ご指摘を踏まえ、これらに加えて、プライベートクラウド、パブリッククラウドについての記載を追記いたします。	1.1.1(5) 「しかし（2）で示したように、今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている。また、それぞれのサービスは、必ずしも一社で提供するとは限らず、複数のクラウドサービス事業者が相互に連携して提供されることも多くなっている。」	1.1.1(5) 「しかし（2）で示したように、今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている。また、プライベートクラウド、パブリッククラウド、ハイブリットクラウドなど、多様な実現形態が存在している。加えて、それぞれのサービスは、必ずしも1社で提供するとは限らず、複数の事業者が相互に連携して提供されることも多くなっている。」
5	アマゾンウェブサービスジャパン株式会社	法人	GL	全般	全般	本ガイドラインは、以前に政府機関から公表された他の様々なガイドラインの要求事項を統合して参照しています。そのために多数の要求事項が重複していますが、このように重複して記載することは、クラウドサービス事業者が医療情報を保護するために重要な事項を特定するに際し、有益とは言えません。さらに、以前にオンプレミス・システムを意図して記載された要求事項は、クラウドコンピューティングには直接関係しない場合があることにも留意する必要があります。	医療情報を取り扱うクラウドサービス事業者は、サービス形態によっては、他のガイドラインで定める安全管理対策にも対応することが求められます。 本ガイドラインの改定の検討の中で、事業者の負担軽減のため、関連するガイドラインの引用参照の要望が多く寄せられたことを受けて対応したものでありますので、原案のとおりとさせていただきます。		
6	アマゾンウェブサービスジャパン株式会社	法人	GL	全般	全般	本ガイドラインにおいてISMS等の第三者の認証の取得についての言及がありますが、ISO/IEC 27001, ISO/IEC27002、ISO/IEC 27017および ISO/IEC 27018といった国際標準について明確に言及し、これらを参考にすべきこと、また、これらの国際的な認証によって、本ガイドラインに記載されたクラウドサービス事業者に対する安全管理に関する要求事項を代替できることを記載していただきたいと考えます。これらの国際標準に基づく認証は、客観的な確認項目について第三者が認定しているため、高い信頼を置くことができ出来ますし、これらを参考にすることで、利用しようとするクラウドサービスが一定の望ましい水準にあることを確保できると考えます。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えております。本ガイドラインで、公正な第三者認証を得ることを推奨しておりますが、ご指摘を踏まえ必要な例示を追記させていただきます。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しております。 各種の認証基準を満たすことで満たされる要求事項もありますが、上記のような観点を踏まえ、それぞれの要求事項について再度確認いただき、その対応状況を医療機関等に提示いただくようお願いいたします。	2.4 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証等の公正な第三者の認証等を取得すること必須であると考えられる。」	2.5 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証（注）等の公正な第三者の認証等を取得すること必須であると考えられる。」 （注）ISMSに関する一般的な基準であるJIS Q 27001:2006 (ISO/IEC 27001:2005) に基づく認証のほか、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針であるJIS Q 27017:2016 (ISO/IEC 27017:2015)やパブリッククラウドにおける個人情報保護に関する指針であるISO/IEC 27018:2014に基づく認証等がある。

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
7	アマゾンウェブサービスジャパン株式会社	法人	GL	全般	全般	本ガイドラインは、非常に詳細にクラウドサービス事業者が取る安全管理対策の例を記載し、詳細なSLA参考例及びサービス仕様適合開示書を提示しています。当社は、医療情報が重要な情報であることには同意するものの、医療情報の収集、取扱い、処理および保管に伴うリスクは、アプリケーション、プロセスおよび関連するシステムのセキュリティ設計およびアーキテクチャによって異なります。安全管理について、1つ1つ要件を定めるようなアプローチを取れば、関連するリスクおよび利用可能なリソースを考慮することなく、不必要なコストや人員を追加し、セキュリティについての誤った理解を招き、却って、セキュリティを妨げる可能性があります。このようなアプローチを取るべきではなく、ISO/IEC27001(ISMS)の標準に基づいたリスクベースのアプローチにより、リスクを適切に特定し管理すべきです。 この点、本ガイドラインは、クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれると指摘していますが（本ガイドライン13頁及び脚注13参照）、適用が想定されない項目が明確ではないため、誤解によって本ガイドラインに記載された適用が想定されない安全管理策を行おうとしてしまうことがあり得ます。当該クラウドサービスにはどの安全管理策が重要かについて、医療機関が優先順位を付けることが出来なければ、医療機関にとってクラウドサービスを利用する上での大きな制約になり、クラウドサービスの利用を却って妨げてしまうことを危惧します。従って、前記の国際標準を参照することによって、本ガイドラインを簡潔にすることが可能であって、そのようにすべきと考えます。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えており、本ガイドラインでも、公正な第三者認証を得ることを推奨しております。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しておりますので、厚生労働省ガイドラインをベースとしたアプローチのままとさせていただきます。		
8	アマゾンウェブサービスジャパン株式会社	法人	GL	全般	全般	第3章　クラウド事業者に対する安全管理に関する要求事項 3.2 医療情報サービスに求められる安全管理に関する要求事項　情報技術および情報システムの安全管理については、ISO/IEC27001、ISO/IEC27002、ISO/IEC 27017およびISO/IEC 27018により既に標準化されている管理を参照することによって簡潔にすることができます。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えており、本ガイドラインでも、公正な第三者認証を得ることを推奨しております。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しておりますので、厚生労働省ガイドラインをベースとしたアプローチのままとさせていただきます。		
9	BSA ザ・ソフトウェア・アライアンス	法人	GL	全般	全般	国際標準の重視 本ガイドラインは、2.4において、クラウドサービス事業者が医療情報を取り扱う際に、公正な第三者の認証（例えば、情報セキュリティマネジメントシステム（ISMS））を取得することは、医療機関等に対するクラウドサービス事業者の説明責任を果たす有効な手段であると認識していますが、私どもは、本ガイドライン全体を通して、関連する国際的に認められた標準の重要性をより明確にかつ強調して記載することによって、本ガイドラインがより良いものになると考えます。また、本ガイドライン中のクラウドサービス事業者への要求事項は、国際的に認められた標準の遵守によって満たされ、また、かかる標準で置き換えることが可能である旨、本ガイドラインに明示的に記載することをお奨めします。 ISMS（ISO/IEC27001）の他、そのような国際的に認められた標準の具体例としては、ISO/IEC27017、ISO/IEC27018が挙げられます。これらの標準は、専門家によって策定され、客観的な審査のシステムを採用しています。また、いくつかの国際標準及び関連する認証は、監査によって、サービスプロバイダーが適合することを確実にしています。このように、広く採用されている国際的に認められた標準や関連する認証を用いることで、サービスの安全性を高め、医療機関等も安全性についてより確信を得ることができると考えます。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えており、本ガイドラインでも、公正な第三者認証を得ることを推奨しております。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しておりますので、厚生労働省ガイドラインをベースとしたアプローチのままとさせていただきます。		
10	BSA ザ・ソフトウェア・アライアンス	法人	GL	全般	全般	国際標準の重視 また、私どもは、貴省に対し、このような国際標準の枠組みに従い、かつ、国際標準と一致する用語を用いて、本ガイドラインを策定するようお奨めします。ISMSの他、よりクラウドコンピューティングに適合するように策定された、国際的に認められた標準がいくつかありますので、貴省は、これらを本ガイドラインに明確に取り入れた方が良いと考えられるかもしれません。かかる国際標準の例としては、ISO/IEC 17788 (Cloud computing – Overview and vocabulary)及びISO/IEC 17789 (Cloud computing – Reference architecture)があります。実際、ISO/IEC 27017 は直接この2つの国際標準に言及しています。また、ISO/IEC 19086-1 (Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts)についても、クラウドSLAのガイドラインを作成する際に非常に有益であると思われます。	1.2.1に記載の用語については、本ガイドラインと厚生労働省ガイドラインの整合性を確保するため、原案のとおりとさせていただきます。 1.2.2の用語については、本ガイドラインで特別の定義をする必要があるものを除き、ご指摘を踏まえて修正いたします。	1.2.2 SLA 「クラウドサービスにおけるSLAとは、クラウドサービス事業者とクラウドサービスの利用者が利用契約を締結するにあたり、両者がサービス及びサービスレベルについて合意した内容を明文化したものである。」	1.2.2 SLA 「書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）」
11	BSA ザ・ソフトウェア・アライアンス	法人	GL	全般	全般	規範的なガイドラインではなくハイレベルなガイダンスを策定することの有効性 私どもは、貴省が、革新的なクラウドサービスを利用しながら医療情報を保護するためのガイドラインを提供しようとされる努力に対し、感謝申し上げます。しかしながら、私どもは、過度に詳細かつ規範的な要求事項を課すことは差し控えるべきであり、貴省には、より高度なガイダンスに焦点を当てていただきたいと考えております。詳細で統一的な安全管理の方法を定めることは、医療機関等に大きな負担をかけ、医療情報を使用し、保存し、安全性を高めるのに有益で革新的な信頼できるクラウドサービスの利用に際し、大きな制約を課すことにつながります。また、本ガイドラインでは、パブリッククラウドとプライベートクラウドとの違いが十分に説明されておらず、infrastructure-as-a-service（IaaS）、platform-as-a-service（PaaS）、software-as-a-service（SaaS）といった異なるタイプのクラウドサービスの違いを十分に踏まえて記載されていません。 本ガイドラインは様々な種類のクラウドサービスを網羅するものであって、各クラウドサービスの技術や機能はそれぞれ異なることから、本ガイドラインに記載されているクラウドサービス事業者への安全管理の要求事項はあくまでも参考の目的で記載されているにすぎず、実際に医療機関等が選択するクラウドサービスによっては、多くの対策が該当しないか又は関係しない可能性があることを明記するよう、貴省に対し求めます。	ご指摘の観点については、まず、1.2.2において、「ASP・SaaS」、「PaaS」、「IaaS」を定義し、それぞれクラウドサービスの一つであることを明記しております。また、1.1.1(5)において「今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている」ことを記載しております。 その上で、1.3.2(1)(イ)において、「クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれていることから、各クラウドサービスの内容に照らして、必要な要求事項へ対応することが求められる」ことを明記しており、ご指摘の趣旨は踏まえているものと認識しております。 なお、ご指摘のうちプライベートクラウド・パブリッククラウドについては、ご指摘の趣旨を踏まえ、それぞれ記載するとともに、そういった多様なクラウド配置が有りえることを明記させていただきます。	1.1.1(5) 「しかし（2）で示したように、今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている。また、それぞれのサービスは、必ずしも一社で提供するとは限らず、複数のクラウドサービス事業者が相互に連携して提供されることも多くなっている。」	1.1.1(5) 「しかし（2）で示したように、今日ではASP・SaaSのほか、PaaS、IaaS等、様々なレイヤーのクラウドサービスが提供されている。また、プライベートクラウド、パブリッククラウド、ハイブリットクラウドなど、多様な実現形態が存在している。加えて、それぞれのサービスは、必ずしも1社で提供するとは限らず、複数の事業者が相互に連携して提供されることも多くなっている。」
12	BSA ザ・ソフトウェア・アライアンス	法人	GL	全般	全般	2.「第3章 クラウドサービス事業者に対する安全管理に関する要求事項」 適切かつ必要な安全管理は、クラウドサービス事業者が採用する技術及び機能並びに医療機関等によるクラウドの利用状況によって異なります。本ガイドラインが様々なクラウドサービスを対象とするものである以上、本ガイドラインに記載されているクラウドサービス事業者に対する安全管理に関する要求事項は、あくまで参考としての記載であり、医療機関等が実際に利用するクラウドサービスによっては、多くの対策が該当しないか又は関連しない可能性があることを明記していただけるようお願いします。 そのように修正することにより、医療機関等は、本ガイドライン中の不合理または該当しない要求事項遵守の要請なく、自らが利用したいクラウドサービスを採用できることを明確に理解するのに役立ちます。	1.3.2(1)(イ)において、「クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれていることから、各クラウドサービスの内容に照らして、必要な要求事項へ対応することが求められる」ことを明記しており、ご指摘の趣旨は踏まえているものと認識しております。		

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
13	個人B	個人	GL	全般	全般	本ガイドラインでは、「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」の参照について 「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」（平成24年10月制定）については、改正個人情報保護法制定（平成25年制定、27年5月施行）の前のガイドラインを参照することについては法的根拠および社会情勢から鑑みて疑問である。 個人情報保護委員会の「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）」（平成28年11月）や、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（Ver5.0）（平成29年5月）などを参照規程とし、どうしても不足があれば、「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」を改版する措置をまって、検討を進めるべきである。	本ガイドラインは、医療情報を取り扱うクラウドサービス事業者に関係する現行ガイドラインを網羅的に参照できるようにすることを目的としております。 「医療情報を受託管理する情報処理事業者」に該当するクラウドサービス事業者は、現行の経済産業省ガイドラインを遵守する必要がありますので、原案のとおりとさせていただきます。		
14	一般社団法人日本画像医療システム工業会	法人	GL	全般	全般	意見：「厚生労働省ガイドライン」で頁や章を参照した場合に版数を指定しておかないと不明確。今後改定があった場合に参照できなくなる可能性がある。 提案する記述文：「第5.版」等、参照すべき版数を明示する。	ご指摘を踏まえて修正いたします。		
15	個人C	個人	GL	P5	1.1.1(5) 脚注3	「3 総務省 ASP医療ガイドラン1.1版においても、ASP・SaaS 事業者以外のクラウドサービスへ適用を排除するものではなく、・・・」 文章の意図が読み取れません。本文の趣旨は理解できますが、この文章はどのような観点から本文を補足しているのでしょうか？	ご指摘の箇所は、ASP・SaaSでないクラウドサービスについて、今回の改定により新たにガイドラインの対象となるわけではなく、これまでもガイドラインの対象であったことを補足するものです。		
16	アマゾンウェブサービスジャパン株式会社	法人	GL	PP7-11	1.2	第1章　本ガイドラインの前提条件及び読み方 1.2 本ガイドラインで用いる用語の定義　使用される用語の整合性を確保し、ISO/IEC17789:2014およびISO/IEC27000などの国際標準を使用してすでに実施されているセキュリティ対策およびシステムの相互運用を可能にするために、技術およびセキュリティの用語の定義は、国際標準に従うべきです。	ご意見を踏まえ、整合性の観点から、1.2.1の厚労省ガイドラインで規定されている用語については、厚労省ガイドラインの定義を利用しつつ、それ以外の用語については、1.2.2として「クラウドサービス提供における情報セキュリティガイドラインで使用されている用語」を新設し、国際標準も踏まえて定義されている「クラウドサービス提供における情報セキュリティ対策ガイドライン第2版」と同じ定義を使い、「クラウドサービス提供における情報セキュリティ対策ガイドライン第2版」に定義のない用語については、1.2.3に「その他の用語」として整理する形に修正いたします。	1.1.1 厚生労働省ガイドラインで使用されている用語 1.1.2 その他の用語	1.1.1厚生労働省ガイドラインで使用されている用語 1.1.2　クラウドサービス提供における情報セキュリティガイドラインで使用されている用語 1.1.3　その他の用語
17	個人E	個人	GL	P9	1.2.2	・今回のガイドラインの中で「PHR」について明確な位置づけが提示されたことは望ましいが、PHRを医療情報のみに限定しまうことに疑問を感じる。本来のパーソナル・ヘルス・レコードという意味では、国民目線で見れば、医療情報のみならず平時のバイタルや活動量などもヘルスレコードでは、と考える。このガイドラインでPHRの定義が示されることによって、「PHR＝医療情報」という認識が定着し、国民目線での個人健康情報サービスを提供する事業者の活動に誤解を与えたり、停滞を招いたり、することを懸念する。PHRはより使いやすく運用されることによって広く国民の理解されるところとなり、結果として国の医療費、社会保障費の抑制に寄与するものではないかと考える。	ご指摘を踏まえて、趣旨が明らかになるように修正させていただきます。	1.2.2 PHR 「患者等が医療情報を自らの判断のもとで活用する仕組み。」	1.2.3 PHR 「個人の生涯にわたる医療・健康等に関するデータを時系列で管理し、本人の判断のもと多目的に活用する仕組み。PHRは、広く個人の健康に関連する様々な情報を活用する仕組みを指すが、本ガイドラインにおけるPHRは、医療情報を活用する場合を対象とする。」
18	個人E	個人	GL	P9	1.2.2	・ガイドラインの中では医療者を起点とした情報を医療情報と位置づけているが、一般的な健康診断などは医療情報であり今回のガイドラインで言うところのPHRに該当する、という理解か？例えば、乳幼児健診は医療従事者が健診を行うが、その情報は自治体に記録保管されるし、小中学校の健診も医療従事者が健診を行うが、教育委員会にて情報が記録管理される、社会人の健診も医療従事者が健診を行った後、国保なら自治体や保健センターに、社保なら協会健保や企業の保険組合にて記録保管される。こうした健康診断情報は要配慮個人情報ではあるが、本人同意によってそれぞれの健診の実施主体から個人へのデータ提供が可能と考えていたが、「医療情報としてのPHR」と位置づけられることにより、医療情報と同等の仕様が求められることになり、サービスの運用コストに反映され、結果として国民にとって有用性の低いPHRになってしまうことを懸念する。	ご指摘のような健康診断の情報を取り扱うクラウドサービス事業者は、本ガイドラインの対象となるPHRサービス事業者に該当します。 ご指摘のような懸念も踏まえ、本ガイドラインでは、「PHRサービスの場合、医療機関等が医療情報を取り扱うクラウドサービスを利用する場合と異なり、患者等が取り扱う医療情報は自らの情報に限られることから、PHRサービス事業者における要求事項への対応は、それに応じた水準・内容となる」ことを明記しておりますので、原案のとおりとさせていただきます。		
19	アマゾンウェブサービスジャパン株式会社	法人	GL	P9	1.2.2	1.2.2　その他の用語 ・IoT機器の定義 IoT機器がインターネットに接続するとの記載は間違いではありませんが、IPアドレスを持つすべての機器が必ずインターネットに接続するというわけでも、その必要があるというわけでもありません。IoT機器については、プライベートネットワークまたはインターネットであり得るTCP/IPネットワークに接続することができる一意のIPアドレスを有するもの、と定義する方がより正確です。	ご指摘の箇所は、当省クラウドセキュリティガイドラインのとおり修正させていただきます。	1.2.2 IoT機器 「IoT機器（デバイス）とは、固有のIPアドレスを持ち、インターネットに接続が可能な機器を指す。センサーネットワークの末端として使われる端末から、コンピューティング機能を持つものまで、エレクトロニクス機器を広範囲にカバーするもの。」	1.2.2 IoT機器 「IoT を構成するネットワークに接続される機器のこと。通信を行う以外の主たる機能としては、計測（センサー）、制御（アクチュエータ）がある。センサー及びアクチュエータは、機器本体と通信・制御部の組み合わせで構成されるものである。ただし、制御部が外部コンピュータとして独立しているものはローカルコンピュータと呼ぶ。」
20	個人B	個人	GL	P9	1.2.2	本文の9ページ「1.2.2 その他の用語」の中の「PHR(Personal Health Record)」について 「患者等が医療情報を自らの判断で活用する仕組み」とあるが、近年の政府（特に厚生労働省・内閣官房等）・諸外国・業界の動向から鑑みて不十分である。 （1）対象は「患者等の医療情報」に限るべきではなく、健常人も含むべきものであるため、「個人の健康に関する情報」を含むことが必須である。 （2）筆者の提言としては、「個人の健康情報・医療情報等を個人の管理下において蓄積された情報。自らの判断のもとで、その情報を利用もしくは必要な相手に提供を行える仕組み。」と考える。 （3）なお、筆者が理事を務める「（一社）PHR協会」では、「PHR協会が考えるPHRの定義」を数年前から下記に掲載しているので参照されたい。 http://www.phrj.org/「phr協会が考えるphrの定義」	ご指摘のように、いわゆるPHRには、「個人の健康に関する情報」を取り扱う仕組みもあると認識しておりますが、本ガイドラインでは、クラウドサービス事業者における医療情報の安全な取扱いの確保という本ガイドラインの策定の目的を踏まえ、いわゆるPHRのうち本ガイドラインの対象となるものを限定することを目的として定義しておりますので、一般的にPHRを定義しようとするものではありません。 ご指摘を踏まえて、上記の趣旨が明らかになるように修正させていただきます。	1.2.2 PHR 「患者等が医療情報を自らの判断のもとで活用する仕組み。」	1.2.3 PHR 「個人の生涯にわたる医療・健康等に関するデータを時系列で管理し、本人の判断のもと多目的に活用する仕組み。PHRは、広く個人の健康に関連する様々な情報を活用する仕組みを指すが、本ガイドラインにおけるPHRは、医療情報を活用する場合を対象とする。」
21	個人B	個人	GL	P9	1.2.2	「1.2.2 その他の用語」の中の「PHRサービス」について 「PHRを提供するクラウドサービス」とあるが、現在は、PHRを提供するには、まず、PHRを取得・蓄積する仕組みが必要である。また、5月25日より施行された次世代医療基盤法もPHRサービスの定義には念頭に置くべきである。従って、「取得・蓄積する仕組み」及び「匿名化／匿名加工情報化」も明記するべきである。 （1）筆者の提言としては、「a.PHRを取得・蓄積するサービス、b.必要に応じてその情報を匿名化／匿名加工情報化するサービス。および、c.当該の実名PHR及び匿名化／匿名加工情報化されたPHRをPHRの本人もしくは第三者に提供するサービス。」と考える。 （2）なお、筆者が理事を務める「（一社）PHR協会」では、「PHRサービス」の内容について、早々に検討する計画である。	本ガイドラインでは、PHRを「患者等が医療情報を自らの判断で活用する仕組み」として定義しているため、取得・蓄積は本ガイドラインにおけるPHRサービスの中に含まれるものと認識しています。 また、ご指摘のように、いわゆるPHRサービスの中には、匿名化／匿名加工情報化を行うサービスもあると認識しておりますが、本ガイドラインは、医療情報を取り扱うクラウドサービスにおけるセキュリティを確保することを目的としているため、匿名化/匿名加工情報化に関する要求事項は設けておりません。なお、別の意見によりPHRの定義を「個人の生涯にわたる医療・健康等に関するデータを時系列で管理し、本人の判断のもと多目的に活用する仕組み」に修正する予定ですが、その場合でも同様と考えています。		
22	アマゾンウェブサービスジャパン株式会社	法人	GL	P10	1.2.2	・IPSecの定義 IPSecは一連のプロトコルであることに留意する必要があります。RFC6071（https://tools.ietf.org/html/rfc6071）のIPSecの定義を使うことをお奨めします。また、IPSecは能力を提供するだけであって、完全性や機密性が実際に実現されるかどうかは、使用する鍵管理システム、システムの運用構成および実装する運用プロセスのサポートなど、他の要因によって異なるため、「実現する」ではなく「提供する」と変更するよう提案します。	ご指摘を踏まえて修正いたします。	1.2.2 IPSec 「暗号技術を使ってIPパケットの完全性や機密性を実現する仕組み。IPパケットの暗号化や認証を行う。」	1.2.3 IPSec 「暗号技術を使ってIPパケットの完全性や機密性を提供する仕組み。IPパケットの暗号化や認証を行う。」
23	アマゾンウェブサービスジャパン株式会社	法人	GL	PP12-19	1.3	1.3 本ガイドラインの対象範囲 本ガイドラインにおける他の箇所でも同様ですが、データ保有者、データ主体、情報管理者、情報処理事業者の概念および原則は、利用者や技術能力の変化に伴い、様々なプロバイダーによるビジネスモデルが常に発展していくものであることから、関係する様々な事業者の役割および責任をより明確に定義して記載されるべきです。	クラウドサービスには、様々な形態が想定され、事業者の役割や責任を一概に定義することが困難であるため、原案のとおりとさせていただきます。		

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
24	個人C	個人	GL	P12	1.3.1(2) 図2	「図2　本ガイドランにおける医療情報の管理主体」 この図の意図が理解できません。文章だけで十分と思われますが、この図で重要な点はなんでしょうか？	ご指摘の図は、患者等も医療情報の管理主体となることを明らかにするものです。厚生労働省ガイドラインでは、そのガイドラインの性質上、医療機関等だけが管理主体として想定されていたため、本ガイドラインでは、患者等が管理主体となる場合があることを図示しております。		
25	HEASNET	法人	GL	P14	1.3.2(1)(イ)	複数のクラウドサービス事業者でサービスを形成する場合、個々のクラウドサービス事業者においては、本ガイドラインで求められている要求事項について対象外になる項目もあるため、医療機関と合意を行う際に、クラウドサービス事業者において対象外である項目を明示するようにしてはどうか。 例えば、HaaS事業者やIaaS事業者である場合に、p.68に挙げられている”マルウェア等への対策”の項目に対しては、提供範囲外のものとなり対象外である。また、PaaS事業者やSaaS事業者にとって、”外部からの攻撃等への対策”の項目に対して対象外となりうる可能性が高いものが多く、きちんとどの項目に対応しているかを示す必要があると考えられる。	本ガイドラインへの適合状況については、医療機関等に対してサービス仕様適合開示書を提示するスキームとしておりますので、提供するサービスの特性によって対象外となる項目についても、同開示書で提示いただくことを想定しております。 なお、「複数のクラウドサービス事業者でサービスを形成する場合」で、ある事業者が他社のサービスを利用して医療機関等に対してサービス提供する場合には、P14にあるように、他社のサービスも含め全体を一括してサービスを提供することになるので、医療機関等との合意に当たっても、他社のサービスに係る部分を含めてサービス仕様適合開示書を提示し、合意する必要があります。		
26	個人C	個人	GL	P15	1.3.2(1)(イ) 脚注13	「13 例えばIssSの場合には、個人情報閲覧や利用者よる通信経路閲する内容は、サービス特性上、想定されるケースが少ない。・・・」 IaaSの利用の場合は本ガイドラインの適用外であることを明記しているのでしょうか？そうであれば1章でIaaSも含めて解説を行っている意図が不明です。	ご指摘の箇所は、「クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれている」ことの具体例を示したものです。ご指摘のような、IaaSが本ガイドラインが適用されないといった誤解が生じる可能性があることを踏まえて、当該注釈は削除いたします。	1.3.2(1)(イ)脚注 「例えばIssSの場合には、個人情報の閲覧や利用者による通信経路に関する内容は、サービス特性上、想定されるケースが少ない。そのため、このような要求事項への対応は求められない。」	1.3.2(1)(イ)脚注 （削除）
27	一般社団法人日本画像医療システム工業会	法人	GL	P15	1.3.2(1)(イ)脚注13	”IssS”は”IaaS”と修正が必要。	ご指摘のとおり、表記の誤りがありました。 なお、ご指摘の箇所については、他の方の指摘を踏まえて削除しました。		
28	一般社団法人日本画像医療システム工業会	法人	GL	P16	1.3.2(1)(イ)図4	位置を左右合わせる	ご指摘のとおり、修正いたします。		
29	アマゾンウェブサービスジャパン株式会社	法人	GL	P18-19	1.3.2(4)	1.3.2 本ガイドラインが対象とするクラウドサービス（4）PHR(パーソナル・ヘルス・レコード)における適用領域ここで言及されている情報は、依然として個人情報であるため、データ保有者とデータコントローラーの関係のように、データを置いた者（例えば、個人、医療機関、その他）が引き続きその適切な保護を確保する責任を負うべきと考えられ、これらの関係をより整理すべきと考えます。	本ガイドラインではPHRは一次的に患者に管理責任があるものとして、その保存などのプロセスに関する責任分界について、2.4で示しております。ご指摘の趣旨については、これを踏まえてご理解いただければ幸いです。		
30	個人C	個人	GL	P20	1.4 脚注18	「今後は特に・・・本ガイドラインと整理し、必要に応じて、「ASP・SaaSにおける情報セキュリティ対策ガイドライン」を参照することとする。」 「ASP・SaaSにおける情報セキュリティ対策ガイドライン」は参照扱い良いのでしょうか？	従来、クラウドサービス事業者が医療情報を取り扱う際に遵守すべき総務省ガイドラインとしては、本ガイドラインの前身である「総務省ASP 医療ガイドライン」及び「ASP・SaaS における情報セキュリティ対策ガイドライン」（平成20 年1 月）の2つのガイドラインを示してきましたが、今後は特にクラウドサービス事業者が医療情報を取り扱う際に遵守すべきガイドラインは本ガイドラインと整理し、必要に応じて、「クラウドサービス提供における情報セキュリティ対策ガイドライン」（総務省　平成30年7月）を参照することとしております。		
31	個人C	個人	GL	P21	1.4 図7	「医療情報処理受託業務事業者」は「医療機関」と「クラウドサービス事業者Aが提供するアプリケーション」の間に位置するのではないでしょうか？この図では、「医療機関」が「クラウドサービス事業者」を直接指定して、「医療情報処理委託業務事業者」に「クラウドサービス事業者A」に委託する図に読み取れます。このような契約形態は存在しないように思えます。また、「医療情報処理受託業務事業者」が存在すれば、クラウドサービス事業者A～Cは経済産業省ガイドラインに準拠する必要はないと読み取れる図になっているが、良いでしょうか？	ご指摘を踏まえて修正いたします。	1.4 図7 	

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
31	個人C	個人	GL	P21	1.4 図7				
32	BSA ザ・ソフトウェア・アライアンス	法人	GL	PP25-37	2.2 2.3	1.「2.2 クラウドサービス事業者と医療機関等の管理者との責任分解の考え方」及び「2.3　医療情報の管理におけるクラウドサービス事業者の責任」 本ガイドラインでも指摘するとおり、パブリッククラウドの利用に当たっては、医療機関等とクラウド事業者の間で責任分担することは重要であり、クラウドサービス事業者と医療機関等の管理者との間で、責任分界点について合意することが必要です。しかしながら、その責任分界点はサービスの提供形態（IaaS, PaaS, SaaSなど）によって大きく変わらざるを得ません。本ガイドラインは、様々なクラウドサービスを対象とするものである以上、サービスの形態や性質によって責任分界点も変わることを明記していただきたいと考えます。	1.3.2(1)(イ)において、「クラウドサービスの内容によっては、本ガイドラインの一部項目の適用が想定されないものも含まれていることから、各クラウドサービスの内容に照らして、必要な要求事項へ対応することが求められる」ことを明記しています。 その上で2,3,3において、具体的な責任の内容や責任分界点は、医療機関等や関係するクラウドサービス事業者と合意するものとして記載しているため、ご指摘の趣旨は踏まえているものと認識しております。		
33	アマゾンウェブサービスジャパン株式会社	法人	GL	PP31-34	2.3.3	プライベートクラウド、パブリッククラウド又はそのハイブリッドかというクラウドサービスの形態の違い、IaaS、PaaS、SaaS等のクラウドサービスの種類の違いによって、当該サービスにおける責任分界点は異なります。従って、本ガイドラインにおいても、その利用するクラウドサービスの形態や種類によって、多様な責任分界点がある事にも言及いただくようお願い致します。	2,3,3では、複数のクラウドサービス事業者が関わる場合の医療機関等との責任関係を示しておりますが、具体的な責任の内容や責任分界点は、医療機関等や関係するクラウドサービス事業者と合意するものとして記載しているため、ご指摘の趣旨は踏まえているものと認識しております。		
34	HEASNET	法人	GL	P35	2.3.3(2)	"この場合、基本的には医療機関等が、各クラウドサービス事業者と取り決めることになるが、AとBのシステム上の機能連携を行うのに必要な対応や、障害時における責任分界点を明示するのに必要な情報提供等を行うことがA及びBに求められる。"とあるが、責任分界点がAでもなく、Bでもない事項が存在する場合は、医療機関等において必要な対応をとるように明示した上で合意する必要がある旨を記載してはどうか。責任分界点がAでもBでもない事例としては、例えば、医療機関等とAが契約を行いPaaSまで構築(ウィルス対策ソフトは対象外)し、医療機関等とBがアプリケーションのみの構築を担当した場合に、ウィルス対策ソフトの導入に関する責任分界は医療機関等となる。そのため、AとBに対応や情報提供等を求めているが、医療機関等も含めて、責任分界点等の調整を行い合意する必要がある。このため、下記のように修正してはどうか？ 【修正後】 "この場合、基本的には医療機関等が、各クラウドサービス事業者と取り決めることになるが、AとBのシステム上の機能連携を行うのに必要な対応、ならびに障害時における責任分界点に関する必要な情報提供等を行うことがA及びBに求められ、これらの情報を基に医療機関等を含めA及びBが調整し、合意する必要がある。"	ご指摘を踏まえて修正いたします。	2.3.3(2) 「この場合、基本的には医療機関等が、各クラウドサービス事業者と取り決めることになるが、AとBのシステム上の機能連携を行うのに必要な対応や、障害時における責任分界点を明示するのに必要な情報提供等を行うことがA及びBに求められる。」	2.3.3(2) 「この場合、基本的には医療機関等が各クラウドサービス事業者と取り決めることになるが、AとBは、医療機関等に対して、AとBの情報システムの機能連携に必要な対応、障害時における責任分界点等に関する必要な情報提供を行うとともに、これらの情報に基づいて医療機関等を含めて調整し、合意する必要がある。」
35	アマゾンウェブサービスジャパン株式会社	法人	GL	P38	2.4	2.4　医療情報に関わるクラウドサービス事業者に関連する第三者認証の考え方 安全を確保するために別個の認証を要求するのではなく、ISO/IEC27001(ISMS)認証取得を評価している点は良いと考え、賛同します。クラウドサービスプロバイダーにとっては、プライバシーマークの認証の代わりに、ISO/IEC27001(ISMS)認証の拡張でアドオン認証であるISO27018を、必要なプライバシー確保のために取得することが有用です。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えております。本ガイドラインで、公正な第三者認証を得ることを推奨しておりますが、ご指摘を踏まえ必要な例示を追記させていただきます。	2.4 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証等の公正な第三者の認証等を取得すること必須であると考えられる。」	2.5 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証（注）等の公正な第三者の認証等を取得すること必須であると考えられる。」 （注）ISMSに関する一般的な基準であるJIS Q 27001:2006 (ISO/IEC 27001:2005) に基づく認証のほか、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針であるJIS Q 27017:2016 (ISO/IEC 27017:2015)やパブリッククラウドにおける個人情報保護に関する指針であるISO/IEC 27018:2014に基づく認証等がある。

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
36	個人 F	個人	GL	P38	2.4	■ 原文： 医療情報は特に高い注意義務による保護を要することから、クラウドサービス事業者が医療情報を取り扱う際に、公正な第三者の認証を取得することは、医療機関等の管理 者に対しシステムや運用情報等の説明責任を果たす際に有効な手段であると考えられる。 そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証等の公正な第三者の認証等を取得すること必須であると考えられる。これ以外のクラウドサービス事業者の場合においても、プライバシーマーク認定を取得することが強く求められる。また、不足なく適用範囲を定めた適用宣言書に基づくISMS 認定の取得を考慮することも求められる。 なお、保健医療福祉分野においては「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)」20が策定されている。医療情報を取り扱うクラウドサービス事業者がプライバシーマーク認定を取得する際には、この認定指針を参照し、準拠に努めることが望まれる。 ■ 意見： 情報処理事業者によるプライバシーマーク認定、ISMS認定等の第三者認証取得を必須にすることに賛同いたします。但し、これら認定・認証は機微な医療情報を扱う事業者としての認証としては必ずしも十分ではないと思われます。また今後グローバルに活躍できる企業の育成も見据え、事業者としての信頼度向上を計れるグローバル標準の認証取得を考慮すべきだと考えます。 ISO/IEC27017やISO/IEC27018の認証取得、SSAE16の監査報告書の提示、等の推奨を提案いたします。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えております。本ガイドラインで、公正な第三者認証を得ることを推奨しておりますが、ご指摘を踏まえ必要な例示を追記させていただきます。	2.4 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証等の公正な第三者の認証等を取得すること必須であると考えられる。」	2.5 「そのため、クラウドサービス事業者が情報処理事業者の場合には、プライバシーマーク認定・ISMS 認証（注）等の公正な第三者の認証等を取得すること必須であると考えられる。」 （注）ISMSに関する一般的な基準であるJIS Q 27001:2006 (ISO/IEC 27001:2005) に基づく認証のほか、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針であるJIS Q 27017:2016 (ISO/IEC 27017:2015)やパブリッククラウドにおける個人情報保護に関する指針であるISO/IEC 27018:2014に基づく認証等がある。
37	MITSF（メディカルITセキュリティフォーラム）	法人	GL	PP40-123,155-170	3.2全般, 3.6.2全般	【リスク／対策に関する整理について】 「ガイドラインに基づくSLA参考例及びサービス仕様適合開示書」の3.1「リスク評価」における「本項を定める上での考え方」には以下の記載がある。 “クラウドサービスを利用し、医療情報を取り扱う場合には、クラウドサービス事業者は、医療機関等が行うリスク分析に対応する形で対策を講じることが求められる。したがって、クラウドサービス事業者においても、医療情報を取り扱う際のリスク評価を行い、これに応じた安全対策が求められ、その内容は医療機関等が定める内容を満たしていることが必要である” また、4．3．1「サービスレベルにみあったコストと提案」には、以下の記載がある。 “したがって、第一にクラウドサービス事業者は、情報セキュリティ対策ガイドライン及び本ガイドラインに示す対策及び対応内容を遵守しながらサービスを提供することが求められ、医療機関等との協議により合意する契約、SLA等の内容もこれを満たすものであることが必要である” 上記の記載からは、クラウド事業者はリスク評価の結果に基づき、3．2「医療情報サービスに求められる安全管理に関する要求事項」で定められた対策群について、リスクの重要度の観点より、医療機関と合意可能な合理的な対策を選択的に講じることが求められていると考えられる。 つまり、リスク評価の結果に基づき対策の重要度・優先度を精査し、事業者と医療機関の合意の下で、合理的な対策の実施が求められるという枠組みが示されていると考える。 しかしながら、3．2「医療情報サービスに求められる安全管理に関する要求事項」には、要求事項がチェックリスト型で列記されるのみであり、どの対策がどのようなリスクを前提としており、その観点から最低限実施すべき事項（厚労省ガイドラインのC項に該当）で、どれが推奨事項（D項に該当）なのかが明確でない。 評価すべきリスクは各医療機関の環境要因によりもちろん異なるが、リスクシナリオの観点から一定のパターンに定型化して例示することは可能である。 （厚労省ガイドラインの第6章-2：ISMSの実践では一定のパターンを例示している） また、最低限実施すべき事項のなかには、対策の性質、例えばリスクの顕在化を防止する予防的対策、リスクの顕在化を早期検知し、被害の拡大防止・極小化を行う発見的・復旧的対策が混在している。 リスクの内容によって、対策の性質を勘案して、複合的な組み合わせの下で合理的な対応を図ることはリスクマネジメントの基本であるが、こうした観点から要求事項の整理が行われていない。 これは3．6．2「PHR サービス事業者を適用対象とする要求事項」も同様である。 よって、以下を提言する （1）3．2「医療情報サービスに求められる安全管理に関する要求事項」、3．6．2「PHR サービス事業者を適用対象とする要求事項」における各要求事項が想定するリスクを明確化すること。そのうえで、想定されるリスクに対して最低限の要求事項／推奨事項を明確にすること。 （2） 各要求事項の対策の性質（予防的/発見的/復旧的）を明確化し、その組み合わせによりリスクを合理的に低減するアプローチの重要性を明示すること。	本ガイドラインは、医療機関等が本来果たすべき責務の一部を受託するクラウドサービス事業者に対する要求事項を示しており、厚生労働省ガイドラインで医療機関等に求められる要求事項を踏まえた内容としています。したがって、本ガイドラインでは、厚労省ガイドラインで想定されるリスクと同様のものを前提として各要求事項を定めておりますので、各要求事項が前提とするリスクについては、厚生労働省ガイドラインをご参照ください。また、PHRサービスについても、医療情報を取り扱うため、医療機関等向けサービスと同様のリスクを想定して要求事項を定めています。		
38	MITSF（メディカルITセキュリティフォーラム）	法人	GL	PP40-123	3.2全般	【リスク管理方針の整理について】 3．2「医療情報サービスに求められる安全管理に関する要求事項」で列記される諸事項は基本的にリスクを受容可能な水準まで低減する管理対策、つまり、リスク低減に係る対策となっている。 リスク管理のアプローチには、リスク低減のみでなく、リスク移転やリスク受容等も含まれ、本来、クラウド事業者は経営体力等も勘案し、低減できないリスクがあればその点を明確化すること、または低減できないリスクを移転することで対応する等、リスク管理方針を医療機関に明確に開示した上で、医療機関は当該方針を勘案の上、事業者の選別を行うことが合理的であり、本来あるべき説明責任の遂行である。 実施事項にリスク低減策のみを列挙し、クラウド事業者に求めても、内部的には実施する体力がないも関わらず、対策を実施していると強弁し、実施状況が確認できる資料を提示するよう要求しても営業秘密を盾にしてのらりくらりと逃げようとする事業者を確実にマネジメントすることは困難である。 上記理由により、以下の点を提言する。 （1） リスク低減策のみでなく、リスク移転、リスク受容等を事業者が選択可能であることを明示化すること。 （2） 医療機関等は事業者のそのようなリスク管理方針（経営方針）をしっかり吟味した上で、事業者選定を行うことの重要性を明示化すること。	ご指摘のうち、(1)については、以下の理由から、原案のとおりとさせていただきます。 ・本ガイドラインはクラウドサービス事業者が医療機関等から受託した医療情報の安全確保を目的としているため、クラウドサービス事業者の判断でリスクを受容することは適当でないこと。 ・同様の理由から、クラウドサービス事業者に対して、損害保険などの金銭的なリスク移転について推奨することは適当ではないこと。 ・金銭的リスク以外のリスク移転は、SLAによる医療機関との合意や再委託といった方法が考えられるところ、それぞれについて実施可能であることは、本ガイドライン上明らかであること。 (2)については、医療機関等に求められる対応であるため、厚生労働省ガイドラインで定められるべき事項であり、また実際に定められているものと認識しておりますが、ご指摘を踏まえ、その重要性の認識を高めるために、必要な記載を追記させていただきます。	4.1 （追記）	4.1 「そこで、医療機関等が、サービスの本ガイドラインへの適合状況を容易に確認することができるとともに、クラウドサービス事業者と医療機関等が容易に合意形成することができるようなスキームが求められる（注）。」 （注）厚生労働省ガイドライン第5版は、医療機関等の管理者に対して、「委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要があり、契約事項に含める」ことを求めているため、その点でも、医療機関等が、サービス内容の本ガイドラインへの適合状況を容易に確認することができるようにすることが重要である。

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
39	MITSF（メディカルITセキュリティフォーラム）	法人	GL	PP40-123	3.2全般	【取り扱われる情報の重要度に応じた対策の整理について】 3．1．1「厚生労働省ガイドラインにおける安全対策の考え方の概要」では、法定保存義務の有無によって、厚労省GLの第6章適用範囲のデータと第7章～9章の適用範囲のデータが整理されている。 しかしながら、3．2「医療情報サービスに求められる安全管理に関する要求事項」の項目では、これが混在するかたちで記述されており、非常に見分けがつきにくい。 3．2．3「技術安全管理対策」では、”厚生労働省ガイドラインでは「e-文書法の対象となる医療情報を含む文書等の作成における真正性の確保」、（・・・）対策が示されている。いずれも外部保存を行うための追加的な要件として示されているものであるが、クラウドサービスにおいては、外部保存による対応ができるものが中心であることから、技術的安全管理対策として規定した”との記述があるが、厚労省ガイドラインの第7章が対象とする文書と第8章（外部保存）が対象とする文書は完全には一致していない。 例えば、以下の文書は厚労省ガイドライン第5版の第7章の対象文書には含まれないが、第8章の対象文書には含まれている。 つまり、外部保存通知のみが適用される文書である。 ・医療法（昭和23 年法律第205 号）第21 条、第22 条及び第22 条の2 に規定されている診療に関する諸記録及び同法第22 条及び第22 条の2 に規定されている病院の管理及び運営に関する諸記録 ・高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準（昭和58 年厚生省告示第14 号）第9 条に規定されている診療録等 ・高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準第28 条に規定されている調剤済みの処方せん及び調剤録 この観点に立つと、上記の診療録等について、3．2「医療情報サービスに求められる安全管理に関する要求事項」のいずれが適用されるべきかについて説明が不十分であり、且つ、分かりにくい。本来的には、クラウド事業者に預託されるデータの種別を中心とした観点より整理した上で、データ管理上の要求事項を明確化すべきである。 上記理由より、以下を提言する。 （1） クラウド事業者に預託するデータの種別に応じて、実施すべき事項を明確に整理すること。可能であれば、取り扱われるデータと対策のマッピング表を整理すること。 （2） 実施すべき事項（対策）は、リスク評価の結果に基づくかぎり、想定されるリスクを前提としている。よって、想定されるリスクを前提として、各対策がどのリスクに紐づくかを明確化すること。 （3） 各対策にはその性質によって、キーとなる重要な対策（キーコントロール）、及び当該キーコントロールが機能不全であっても、補完的にリスクを低減できる対策（補完的コントロール）が存在するため、その関係性を整理すること。	ご指摘のとおり、厚生労働省ガイドラインでは、第6章で医療情報の取扱い全般に関する安全管理対策を示すとともに、第7章で保存義務のある診療録等を電子的に保存する場合の安全管理対策、第8章で保存義務のある診療録等を医療機関等の外部に保存する場合の安全管理対策、第9章でe-文書法に基づいてスキャナ等により電子化して保存する場合の安全管理対策を付加的に示しています。 その一方で、厚生労働省ガイドラインでは、保存義務がない文書等であっても、個人情報の保護について留意しなければならない文書等について、バックアップ情報等を含めて、それらを破棄せず保存している限り、7 章及び 9 章に準じて取り扱う必要があるとしています。また、法定保存年限を超過する等により、保存義務がなくなった診療録等を外部保存する場合も、8章に準じて取り扱う必要があるとしています。 このように、厚生労働省ガイドラインでは、法定保存義務のない医療情報であっても、法定保存義務のあるも医療情報と同等の真正性・見読性等を確保することが求められていることを踏まえ、本ガイドラインでは、その趣旨がより明確になるよう、「3．2 医療情報サービスに求められる安全管理に関する要求事項」において、全ての医療情報に求められる安全管理対策を掲載しつつ、その中で特に法定保存義務がある医療情報に求められる安全管理対策についてはその旨記載するとともに、「3．3 外部保存に関する要求事項」において、法定保存義務のある医療情報に求める安全管理対策の記載場所を一覧にして記載する形としております。 上記のとおり、ご指摘のデータの種別に応じた対策の明確化は既に実施しているものと認識しておりますので、原案のとおりとさせていただきます。 また、ご指摘のうちリスクの明確化については、厚生労働省ガイドラインで想定されるリスクと同様のものを前提として各要求事項を定めておりますので、各要求事項が前提とするリスクは、厚生労働省ガイドラインをご参照ください。 加えて、ご指摘のうちキーコントロールについては、クラウドサービス事業者が採用する対応方策によって変わるものであり、クラウドサービス事業者が行うリスク分析の結果を踏まえて整理されるべきものでありますので、ガイドラインで一律的な対応を示すことは適切でないと考えております。		
40	アマゾンウェブサービスジャパン株式会社	法人	GL	P40	3.2.1(1)	3.2.1 組織的安全管理対策 6.3 C 1. 担当者の限定については、管理が確実に実施され、実際に運用できるよう、目標を明確にする必要があります。	ご指摘の箇所は、厚生労働省ガイドラインで規定される医療機関等に対する要求事項を引用したものであり、本ガイドラインで新たに規定する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。		
41	アマゾンウェブサービスジャパン株式会社	法人	GL	PP42-45	3.2.1(2)	3.2.1 組織的安全管理対策(2)クラウドサービス事業者への要求事項 ここに記載されている事項は、それぞれ、ISO/IEC27017およびISO/IEC27018で既に標準化されているセキュリティおよびプライバシー管理を参照することにより、簡潔にすることができます。そして、他の項において記載されているクラウドサービス事業者への要求事項についても、可能な限り前記のISO規格を参照すべきです。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えており、本ガイドラインでも、公正な第三者認証を得ることを推奨しております。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しておりますので、厚生労働省ガイドラインをベースとしたアプローチのままとさせていただきます。		
42	個人A	個人	GL	P42	3.2.1(2)(ア)②	「クラウドサービス事業者において、情報システムについての管理責任を有する責任者（システム管理者）を設置する。」 とあるが、この責任者に求められる具体的資質およびその確認方法が記載されていない。言うなれば全くの未経験者であっても責任者と指定すればガイドラインに適合してしまう。これを防止するため下記の追加を提案する。 ・経済産業省の「情報セキュリティサービス基準」を参照しp6「4．セキュリティ監視・運用サービスに係る審査基準」をクラウドサービス事業者は自ら満たすべきであり、要求事項として追加を提案する。 ・さらに情報セキュリティマネジメント体制が整備されている事を担保するため、ISMSクラウドセキュリティ認証（ISO/IEC 27017）の取得も求められる。 ・責任者個人に求められる資質として、p11「4．セキュリティ監視・運用サービスに関する附則 」に例示される「情報処理安全確保支援士」などの資格を追加するべきである。 この資格は政府IT入札要件、内閣官房情報通信技術(IT)総合戦略室と総務省行政管理局の定める「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第3編第6章 調達）」のP44、P91、P92にも要件として示されている。	責任者に求められる要件を明らかにするため、ご指摘を踏まえて修正いたします。 なお、ISO/IEC 27017の取得については、2.4において第三者認証を取得を要求・推奨しており、ご指摘の趣旨は踏まえているものと認識しております。（クラウドサービス事業者によって、どの認証が適切かは異なると考えられるため、取得を要求・推奨する第三者認証は限定していません。）	3.2.1(2)(ア)② 「クラウドサービス事業者において、情報システムについての管理責任を有する責任者（システム管理者）を設置する。」	3.2.1(2)(ア)② 「情報システムについての管理責任を負い、これについて十分な技術的能力及び経験（注）を有する責任者（システム管理者）を設置する。」 （注）十分な技術的能力及び経験には、例えば情報処理安全確保支援士等の情報セキュリティに関する資格を有し、情報セキュリティに係る技術的対策の実務を一定年数以上経験していることなどが想定される。
43	HEASNET	法人	GL	P42	3.2.1(2)(イ)1.①	「契約には、守秘義務違反に対してはクラウドサービス事業者にペナルティを課すこと、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。」 本項は、クラウドサービス事業者が自身として、約款等においてペナルティを課すことを求めるものか確認したい。 また、一般論としてクラウドサービスの契約は約款型となることが多く、複数の利用者である医療機関等に対して、クラウドサービス事業者からは自身で定めた事項を提示し、内容に対して合意した際に契約に至るものと考えられるため、医療機関等による監督については直接的な監督以外にもクラウド事業者からのレポート提供を受けるなどの方法が考えられるのではないか。	ご指摘の箇所は、守秘義務違反があった場合に、医療機関等がクラウドサービス事業者にペナルティを課すことについて、あらかじめ契約で定めておくよう求めるものです。 また、ご指摘のうち、監督の具体的方法については、一般論として様々な方法が考えられますが、クラウドサービス事業者と医療機関等の間で合意すべき事項であり、ご指摘のような方法だけを取り上げて本ガイドラインで例示することは適切ではないため、原案のとおりとさせていただきます。		
44	個人C	個人	GL	P42	3.2.1(2)(ア)②	「情報システム」は第2章までに出ていない語句です。表現を統一してください。アプリケーション、プラットフォーム、インフラのことでしょうか？これ以降の文章も同様です。	情報システムは、アプリケーション、プラットフォーム、インフラ等を含めた電磁的情報を取り扱う仕組み全般を指して使用しております。情報システムという用語は、厚生労働省ガイドラインにおいても一般的用語として使用されており、本ガイドラインで別途定義することは適切ではないことから、本ガイドラインでも一般的な用語として使用いたします。 なお、表現の統一については、全般的に必要な修正をしております。		

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
45	HEASNET	法人	GL	P44	3.2.1(2)(ウ)7.①	"①医療機関等で患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。"とあるが、患者等への説明の際に医療機関等と合意する意ではないことを明確にするため、下記のように修正してはどうか？ 【修正後】 ①医療機関等が患者等への説明及び同意を得る際に患者に提示することとなる、事業者が提供する情報の範囲並びに事業者の役割等の内容について、サービス仕様適合開示書に基づき、クラウドサービス事業者は医療機関等と合意する。	ご指摘を踏まえて修正いたします。	3.2.1(2)(ウ)7.① 「医療機関等で患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。」	3.2.1(2)(ウ)7.① 「医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。」
46	個人A	個人	GL	P44	3.2.1(2)(ウ)8.	p44「運用管理規程についての要求事項」の「監査」の項目について ・ISMSクラウドセキュリティ認証（ISO/IEC 27017）の取得と維持。 ・情報セキュリティの監査を定期的に実施する事、 そして実施者は「情報セキュリティサービス基準」の「情報セキュリティ監査サービスに係る審査基準」を満たすことを要求する。	以下の理由から、原案のとおりとさせていただきます。 ・ISO/IEC 27017の取得については、2.4において第三者認証を取得を要求・推奨しており、ご指摘の趣旨は踏まえているものと認識しております。（クラウドサービス事業者によって、どの認証が適切かは異なると考えられるため、取得を要求・推奨する第三者認証は限定していません。） ・定期的な監査については、医療機関等との合意に基づいて定期的に実施することを想定して、ご指摘の箇所の③を設けております。 ・「情報セキュリティサービス基準」、「情報セキュリティ監査サービスに係る審査基準」は、セキュリティ監査をサービスとして提供する事業者の基準であり、本ガイドラインで要求事項とすることは適当でないと考えています。		
47	個人C	個人	GL	P45	3.2.1(2)(エ)3.①	「医療情報は、死者に関する情報についても個人情報に準じて・・・・」 厚生労働省のガイドラインでは死者の情報の取扱に対する要求はありません。 （エ）では医療情報へのアクセス管理等の要求について書かれているにも関わらず、ここで死者の取扱がでるのは非常に不自然に思えます。	死者に関する情報については、「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、「死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。」とされています。 クラウドサービス事業者においても、同ガイダンスに沿って医療情報（医療情報は全て個人情報に該当します。）を取り扱わなければならないところ、クラウドサービス事業者が、死者の情報について、遺族等の生存する個人に関する情報にも該当するかを判断することは困難であり、適切でもないため、本ガイドラインでは、死者に関する情報も、個人情報保護法に準拠して管理することを求めることとしています。 当該要求事項は、改定前のガイドラインにおいても求められており、その必要性は現在も変わらないと考えられることから、原案のとおりとさせていただきます。 なお、ご指摘の箇所は、委託契約で個人情報の取扱いを明確にすることを要求する事項の記載箇所でありますので、適切な箇所であると認識してます。		
48	個人D	個人	GL	P46	3.2.2(1)	6．4　C項の2．の1行目「でき る」と、同2行目「出来 ない」とは、文言の統一が必要です。	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.2(1) 6.4 C項2. 「個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。」	3.2.2(1) 6.4 C項2. 「個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることができない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。」
49	HEASNET	法人	GL	PP47-52	3.2.2(2)	(ア)医療情報が物理的に保存されている機器、媒体の設置場所等における物理的安全対策としての要求事項 (イ)個人情報が参照可能な運用端末等の設置場所等における物理的安全対策としての要求事項 (ウ)医療情報を取り扱うクラウドサービスに供する機器等が保存されている建物、部屋対する物理的安全対策としての要求事項 (エ)個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 と分類されているが、医療情報と個人情報と用語が混在しており、混乱を招くおそれがある。 全てが医療情報でよいのであれば、 ・医療情報が格納されている機器・媒体そのもの・・・(エ) ・その機器・媒体が保存されている設置場所・・・(ア) ・その設置場所が含まれる建物や部屋・・・(ウ) ・上記に関らず医療情報が参照可能な運用端末等の場所・・・(イ) という理解でよいか、確認したい。 加えて、このようにした際の対策項目のうち、対応がとれていないものがあるため、再整理が必要となると考えられる。 例："(ウ)医療情報を取り扱うクラウドサービスに供する機器等が保存されている建物、部屋対する物理的安全対策としての要求事項"の項目のうち、"（ア）3.施設の建築物としての安全対策"に含まれるべきものがある。	ご指摘の箇所の要求事項は、原案では以下のような内容に分けられております。 (ア)→サービスに供する機器の設置場所について (イ)→個人情報が参照可能な端末の設置場所について (ウ)→サービスに供する機器の設置場所へのカメラの設置について (エ)→個人情報が保存されている機器自体について 物理的安全対策について、厚生労働省ガイドラインでは、医療情報ではなく個人情報の管理について規定されていることを踏まえ、用語を個人情報に統一した上で、整理がより明確になるよう項目を整理し直すとともに、それに併せて必要な修正を実施いたします。	3.2.2(2) (ア) 医療情報が物理的に保存されている機器、媒体の設置場所等における物理的安全対策としての要求事項 1.施錠管理 ①～③（略） 2.アクセス制御 ①～⑤（略） 3.施設の建築物としての安全対策 ①、②（略） （挿入） (イ) 個人情報が参照可能な運用端末等の設置場所等における物理的安全対策としての要求事項 1.アクセス制御 ①～④（略） 2.覗き見等の防止 ①、②（略） (ウ) 医療情報を取り扱うクラウドサービスに供する機器等が保存されている建物、部屋対する物理的安全対策としての要求事項 1.カメラによる監視 ①～③（略） (エ) 個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 1.機器・媒体等の所在確認等・施錠 ①～③（略）	3.2.2(2) (ア) サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項 1.施錠管理 ①～③（略） 2.アクセス制御 ①～⑦（略） 3.サービスに供する機器や媒体を保存する施設 ①、②（略） 4.カメラによる監視 ①～③（略） (イ) 個人情報が参照可能な運用端末等の設置場所等における物理的安全管理対策としての要求事項 （削除） 1.覗き見等の防止 ①、②（略） (削除) (ウ) 個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 1.機器・媒体等の盗難・紛失防止 ①～③（略）

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
50	JAHIS	法人	GL	P47	3.2.2(2)	（ア）ならびに（ウ）では、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5版」（平成29年5月）において「個人情報」となっている部分が「医療情報」となっている。 「医療情報」→「個人情報」とし、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」と整合性を取るべきではないでしょうか。	ご指摘のとおり、厚生労働省ガイドラインでは、医療情報ではなく個人情報の管理について規定されておりますので、用語を個人情報に統一した上で、（ア）と（ウ）を統合いたします。	3.2.2(2) （ア）医療情報が物理的に保存されている機器、媒体の設置場所等における物理的安全対策としての要求事項 1.施錠管理 ①～③（略） 2.アクセス制御 ①～⑤（略） 3.施設の建築物としての安全対策 ①、②（略） （挿入） （イ）個人情報が参照可能な運用端末等の設置場所等における物理的安全対策としての要求事項 1.アクセス制御 ①～④（略） 2.覗き見等の防止 ①、②（略） （ウ）医療情報を取り扱うクラウドサービスに供する機器等が保存されている建物、部屋対する物理的安全対策としての要求事項 1.カメラによる監視 ①～③（略） （エ）個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 1.機器・媒体等の所在確認等・施錠 ①～③（略）	3.2.2(2) （ア）サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項 1.施錠管理 ①～③（略） 2.アクセス制御 ①～⑦（略） 3.サービスに供する機器や媒体を保存する施設 ①、②（略） 4.カメラによる監視 ①～③（略） （イ）個人情報が参照可能な運用端末等の設置場所等における物理的安全管理対策としての要求事項 （削除） 1.覗き見等の防止 ①、②（略） （削除） （ウ）個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 1.機器・媒体等の盗難・紛失防止 ①～③（略）
51	アマゾンウェブサービスジャパン株式会社	法人	GL	PP47-52	3.2.2(2)	3.2.2　物理的安全管理対策 ISO/IEC27002は、より包括的な物理的および環境的管理要件を有し、参考として利用できます。これにより、実践において整合性が保たれ、ISO/IEC27001認証を遵守の確保に活用することができます。	ご指摘のような第三者認証は、クラウドサービス事業者におけるセキュリティ確保に有効であると考えており、本ガイドラインでも、公正な第三者認証を得ることを推奨しております。 その一方で、医療情報の重要性の観点からより別途設ける必要がある要求事項があること、医療情報の委託元となる医療機関等が、委託先であるクラウドサービス事業者においても厚生労働省ガイドラインで定める安全管理対策が実施されていることを判断できるようにする必要があることを踏まえ、本ガイドラインでは、国際基準ではなく、厚生労働省ガイドラインを基準に、別途要求事項を整理しておりますので、厚生労働省ガイドラインをベースとしたアプローチのままとさせていただきます。		
52	HEASNET	法人	GL	P47	3.2.2(2)(イ)1.	”④個人情報が参照可能な運用端末等の設置場所には撮影機能を有する機器等の持ち込みを制限する。”とあるが、内部犯行を考えた場合、撮影機能に限定せず、業務遂行に関係のない機器等の持ち込みを制限するとしてはどうか？ また、”(イ)の個人情報が参照可能な運用端末等の設置場所等における物理的安全対策”に限らず、”３．２．２物理的安全管理対策”全体に係る項目として、機器等の持込みに係る制限があるべきと考えられる。 参考に挙げられているように、経産省ガイドラインの記述として、”【7.5.2医療情報処理施設への入退館、入退室等に関する要求事項①実施すス制御べき安全管理策】(8)医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。”とある。	ご指摘を踏まえて、記載場所も含めて修正いたします。	3.2.2(2)(イ)④ 「個人情報が参照可能な運用端末等の設置場所には撮影機能を有する機器等の持ち込みを制限する。」	3.2.2(2)(ア)⑤（挿入） 「サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。」
53	アマゾンウェブサービスジャパン株式会社	法人	GL	PP47	3.2.2(2)1.②	(2)クラウドサービス事業者への要求事項 ア）1．施錠管理 これは、媒体その他ストレージ機器やサーバー等の所在場所に関連する環境のリスクに基づいた対策であるべきです。物理的アクセス制御と相俟って、多層の物理的保護がなされているデータセンターにおいては、サーバラックの施錠を義務付けることは、セキュリティの向上につながらず、却って業務効率を妨げます。従って、適切な管理を選択するためのリスクベースのアプローチ（例えば、ISO27001ISMSの利用）は、優れた業務運営とセキュリティのバランスを確保するために重要かつ不可欠です。	サーバラックへの施錠は、機器等への物理的なアクセス制御を適切に実施するために必要な要求事項であると考えておりますので、原案のとおりとさせていただきます。 なお、経済産業省ガイドラインにおいも、同様の要求事項が規定されています。		
54	HEASNET	法人	GL	P47	3.2.2(2)(ア)2.②	”入退状況の管理を定期的に行う”と記載されているが、「管理」の語義が多様で曖昧であることから、ここでは”入退状況の記録の点検を定期的に行う”とすべき。 また、他の項目においても「点検」や「保存」等、具体的な手続きの実施が求められる箇所で「管理」という表現が用いられているケースが見受けられる。より具体的かつ適切な表現に修正するべきではないか。	厚生労働省ガイドラインにおいても入退「管理」という用語を使用していること、「管理」には入退状況の記録・妥当性の確認など、様々な内容が含まれ、それらを個別に記載することは困難であることから、原案のとおりとさせていただきます。		
55	HEASNET	法人	GL	P51	3.2.2(2)(ウ)表題	誤記 医療情報を取り扱う～建物、部屋対する～ 【修正後】 医療情報を取り扱う～建物、部屋に対する～	ご指摘のとおり、表記の誤りがありました。 なお、ご指摘の箇所については、他の方の指摘を踏まえて削除しました。		
56	HEASNET	法人	GL	P57	3.2.3(2)	誤記 (2)を踏まえ、クラウドサービス事業者は～ 【修正後】 (1)を踏まえ、クラウドサービス事業者は～	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.3(2) 「(2)を踏まえ、クラウドサービス事業者は技術的安全管理対策として、 ・利用者の識別及び認証 ・情報の区分管理とアクセス権限の管理 ・アクセスの記録（アクセスログ） ・不正ソフトウェア対策 ・サービス利用に係る機器等（無線LAN、IoT機器）の利用 等が求められる。」	3.2.3(2) 「(1)を踏まえ、クラウドサービス事業者は技術的安全管理対策として、 ・利用者の識別及び認証 ・情報の区分管理とアクセス権限の管理 ・アクセスの記録（アクセスログ） ・不正ソフトウェア対策 ・サービス利用に係る機器等（無線LAN、IoT機器）の利用 等が求められる。」

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
57	一般社団法人日本画像医療システム工業会	法人	GL	P57	3.2.3(2)	意見：（2）で“（2）を踏まえ”とするのは矛盾がある。 提案する記述文：“（2）”は“（1）”が正しいと思われるが確認の上、修正する。	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.3(2) 「（2）を踏まえ、クラウドサービス事業者は技術的安全管理対策として、 ・利用者の識別及び認証 ・情報の区分管理とアクセス権限の管理 ・アクセスの記録（アクセスログ） ・不正ソフトウェア対策 ・サービス利用に係る機器等（無線LAN、IoT機器）の利用 等が求められる。」	3.2.3(2) 「（1）を踏まえ、クラウドサービス事業者は技術的安全管理対策として、 ・利用者の識別及び認証 ・情報の区分管理とアクセス権限の管理 ・アクセスの記録（アクセスログ） ・不正ソフトウェア対策 ・サービス利用に係る機器等（無線LAN、IoT機器）の利用 等が求められる。」
58	個人C	個人	GL	P58	3.2.3(2)(ア)1.	「システム」＝「情報システム」でしょうか？語句の統一をお願いします。以下同様です。	「情報システム」に統一いたします。		
59	個人C	個人	GL	P58	3.2.3(2)(ア)2.③	医療機関の従事者でも他のシステムで利用しているパスワードを利用しないようにすべきではないでしょうか？	該当箇所は、クラウドサービス事業者が行うべき技術的対策を示したものです。 ご指摘の対応は、医療機関等が自ら定めるべき事項であると考えられますので、原案のとおりとさせていただきます。 なお、ご指摘の箇所は、患者等のパスワードに有効期限を定めることが逆にセキュリティを低下させるおそれがあるため、ただし書きで有効期間の設定の代替措置を設けたものであり、医療機関等において、有効期間の設定に加えて同様の措置を取ることを妨げるものではありません。		
60	HEASNET	法人	GL	P59	3.2.3(2)(ア)3.⑧	利用者である医療機関等のパスワードポリシーのことを指しているのか確認したい。また利用者である医療機関等のパスワードポリシーのことを指しているのであれば、”自社において定めたサービスに関するパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。”とすべきと考えられる。なおこのように考えたとき、他のパスワードに関係する事項と併せて、パスワードを用いる時のルールの項目において整理すべきではないか。	ご指摘の箇所の利用者には、3.2.3(2)(ア)1.③のとおり、医療機関等においてサービスを利用する者のほか、サービスに供するシステムの運用若しくは開発に従事する者又は管理者権限を有する者も含めるため、ご指摘の箇所のパスワードポリシーは、これらの者のパスワードに関するポリシーを指しています。 また、パスワードポリシーには、パスワードを用いるときのルールのほか、パスワードの管理に関する内容も含まれるため、パスワードの管理の項目に記載させていただいております。 表現については、ご指摘を踏まえ、修正させていただきます。	3.2.3(2)(ア)3.⑧ 「自社において定めたパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。」	3.2.3(2)(ア)3.⑧ 「利用者のパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。」
61	HEASNET	法人	GL	P62	3.2.5(2)(ウ)(a)1.①	誤記 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、）入力者及び確定者の識別及び認証に関する仕様 【修正後】 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.3(2)(ウ)(a)1.① 「e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC等の汎用入力端末を利用するサービスにおける以下の仕様について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、）入力者及び確定者の識別及び認証に関する仕様」	3.2.3(2)(ウ)(a)1.① 「e-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様」
62	JAHIS	法人	GL	P64	3.2.3(2)	「その内容な証拠としての記録の正確性に関する対応策等について示している。」 校閲漏れと思われます。例えば、「その証拠性確保のために、記録の正確性に関する対応策等を示している。」のように記載してはいかがでしょうか。	ご指摘を踏まえて修正いたします。	3.2.3(2)(エ) 「アクセス記録が、事後に不正なシステムの利用や情報漏洩が生じた場合の原因究明に必須の記録であることを踏まえ、厚生労働省ガイドラインでは、その内容な証拠としての記録の正確性に関する対応策等について示している。」	3.2.3(2)(エ) 「アクセス記録が、不正な情報システムの利用や情報漏洩が生じた場合の原因究明に必須の記録であることを踏まえ、厚生労働省ガイドライン第5版では、その証拠となる記録の正確性に関する対応策等について示している。」
63	HEASNET	法人	GL	P64	3.2.3(2)(エ)1.④	アクセスログも法定保存年限以上、保存する義務があるという理解でよいか確認したい。アクセスに関する監査の時期等で問題が無い場合は法定年限を超えたとき破棄してもよいと考えられる。個人情報保護法第19条で「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」とされている趣旨から、利用する必要があるとするときはその根拠をご教示願いたい。 なお、診療録の確定した記録に関しては、アクセスログとは別に管理し保管すべきである。	ご指摘の要求事項は、少なくとも法定年限の期間中についてアクセス記録等を保存する義務を定めたものであり、法定年限を超えて保存する義務を定めるものではありません。 「法定年限以上の保存期間を設ける」こととしているのは、医療機関等とクラウドサービス事業者の合意により法定年限を超えて保存する場合を排除しないためであり、その場合の必要性等については医療機関等との合意の中で明らかにすべきものと認識しています。		
64	HEASNET	法人	GL	P65	3.2.3(2)(エ)3.①	同期は”日次以上”ではなく、”日次より短い頻度”とすべきと考えられる。”以上”としたとき、例えば月次でもよいと読め、時刻に関する信頼性が失われる恐れが高まる。	ご指摘を踏まえ表現を修正いたします。	3.2.3(2)(エ)3.① 「アクセスログの記録される時刻の信頼性を確保するために、サービスに供するシステムにおける時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次以上の頻度で行う。」	3.2.3(2)(エ)3.① 「アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。」
65	個人D	個人	GL	P68	3.2.3(2)(カ)1.⑤	・1．の丸数字5の2行目「セキュリティ　センター」は、「セキュリティセンター」の誤記では？	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.3(2)(カ)1.⑤ 「サービスに供するシステムの脆弱性に関する情報をJPCERTコーディネーションセンター（JPCert/CC）、内閣サイバーセキュリティ センター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源等に対して、日次及び必要なタイミングで確認する。」	3.2.3(2)(カ)1.⑤ 「情報システムの脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。」

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
66	個人D	個人	GL	P70	3.2.3(2)(カ)参考	・7．6．6（1）の冒頭 等の「セキュリティゲートェイ」は、「セキュリティゲートウェイ」の誤記では？	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.3(2)(カ)参考 「(1)セキュリティゲートェイ(ネットワーク境界に設置したファイアウォール、ルータ等)を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートェイを設置できない場合は、個々の情報処理装置(サーバ)にて、同様のアクセス制御を行うこと。 (2)セキュリティゲートェイでは、不正なIPアドレスを持つトラフィックが通過できないように設定すること(接続機器類のIPアドレスをプライベートアドレスとして設定して、ファイアウォール、VPN装置等のセキュリティゲートウェイを通過しようとするトラフィックをIPアドレスベースで制御する等)。」	3.2.3(2)(カ)参考 「(1)セキュリティゲートウェイ(ネットワーク境界に設置したファイアウォール、ルータ等)を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置(サーバ)にて、同様のアクセス制御を行うこと。 (2)セキュリティゲートウェイでは、不正なIPアドレスを持つトラフィックが通過できないように設定すること(接続機器類のIPアドレスをプライベートアドレスとして設定して、ファイアウォール、VPN装置等のセキュリティゲートウェイを通過しようとするトラフィックをIPアドレスベースで制御する等)。」
67	JAHIS	法人	GL	P72	3.2.3(2)(ク)2.	3.1がどこを指すのか不明です。参照先があるのであれば明記をお願いします。	ご指摘の箇所は、3.2.1(2)(ウ)4.①の誤りですので、修正いたします。	3.2.3(2)(ク)2.① 「3.1において実施するリスク分析結果に基づき、サービスに供するシステムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、必要なバックアップを行うとともに、その内容を運用管理規程等に含める。」	3.2.3(2)(ク)2.① 「3．2．1（2）（ウ）4．①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。」
68	個人D	個人	GL	P77	3.2.3(2)(コ)脚注25	・注釈の「ガイダンス」は、まだ策定されていないのですか？	パブリックコメント開始時点では策定に至っていなかったため、発出月を空欄とさせていただきました。7月24日(火)に公表されておりますので、修正いたします。	3.2.3(2)(コ)注 IoT機器を含む医療機器のサイバーセキュリティの確保について、「医療機器のサイバーセキュリティの確保に関するガイダンス」（厚生労働省 平成30年〇月〇日）が策定されているので、併せて参照されたい。	3.2.3(2)(コ)注 IoT機器を含む医療機器のサイバーセキュリティの確保について、「医療機器のサイバーセキュリティの確保に関するガイダンス」（厚生労働省 平成30年7月24日）が策定されているので、併せて参照されたい。
69	HEASNET	法人	GL	P84	3.2.5(2)1.②	削除方法として”電磁記録媒体の消磁・物理的破壊等”と記載されており、破壊記録等を提出すると記載されているが、利用者が媒体や機器等を占有する形態でサービスを提供しているのではなく、媒体や機器等を他の利用者と共有するような論理的に構成されたサービスの場合は困難と考えられる。 論理的に構成されたサービスでの対応としては、データの消去が考えられるが、どの程度まで消去すればよいのか、考え方をご教示いただきたい。	ここでの破壊記録等の提出の趣旨は、不要となった医療情報の削除が不可逆的になされたことを客観的に示す資料を、医療機関等に提出すると言う趣旨のものです。 そのため、ご指摘のような論理的に構成されたサービスの場合には、不可逆的に削除・消滅されたことを、医療機関等に対して技術的に保証できる程度が求められます。		
70	HEASNET	法人	GL	P89	3.2.6(2)(ア)	誤記 なお、保守に用いるアカウント管理に関する文書化に関する安全管理対策に関して、～ 【修正後】 なお、保守に用いるアカウント管理に関する安全管理対策に関して、～	ご指摘のとおり、表記の誤りのため、修正いたします。	3.2.6(2)(ア) 「なお、保守に用いるアカウント管理に関する文書化に関する安全管理対策に関して、経済産業省ガイドラインで規定している内容を参考に示す。」	3.2.6(2)(ア) 「なお、、保守に用いるアカウント管理に関する安全管理対策について、経済産業省ガイドラインで規定している内容を参考に示す。」
71	HEASNET	法人	GL	P93	3.2.6(2)(エ)1.	厚生労働省標準規格を受け、改造と保守の項目のみではなく、技術的安全対策の項目にも関連する事項を記載すべき。	厚生労働省ガイドラインにおいて、「システム更新を経ても旧システムで保存された医療情報を確実に利用できるようにしておく」ことを目的として、標準規格の利用が推奨されておりますので、本ガイドラインにおいても、「保守における整合性・継続性確保のための安全管理対策」として記載しました。 本ガイドラインは、冗長性をなくす観点から、出来る限り要求事項を重複させない方針で作成しておりますので、原案のとおりとさせていただきます。		
72	MITSF（メディカルITセキュリティフォーラム）	法人	GL	P106	3.2.8(2)(イ)3.	【要件が不明確な対策の明確化について】 3．2．8：「災害等の非常時対応 についての安全管理対策」-（2）クラウドサービス事業者への要求事項-(イ)災害等の非常時対応について -3.非常時に実施すべき代替措置で言及される「非常時に用いる利用者のアカウント及び非常時用機能」とは具体的に何を意味するのか不明確である。 本文では、「サービス仕様適合開示書に基づき、医療機関等と合意する」と記載もあるが、サービス仕様適合開示書の「本項を定める上での考えかた」にも明確な説明はない。 非常時に用いる利用者のアカウント、非常用機能とは、全ての権限を有し、全ての情報へアクセス可能なスーパーユーザー、あるいはそれを可能とする機能を指すものであれば、曖昧な表現は排し、そのように明記すべきである。 厚労省ガイドラインの第6章-10の災害時などの非常時対応のスキームが、SPC(The Joint NEMA/COCIR/JIRA Security and Privacy Committee)白書の「Break-Glass An Approach to Granting Emergency Access to Healthcare Systems」に準拠しているがゆえに、このような記述になっているかもしれないが、一般のクラウド事業者にはこのような背景も分からず、非常用機能と言われてもそもそも今日の技術環境においてそのような機能要件は様々な具体的な対策（冗長化、仮想化環境におけるリアルタイム切り替え等）により対応されている。 このような観点を踏まえ、3．2．8「災害等の非常時対応についての安全管理対策」における「非常時に用いる利用者のアカウント」、「非常用機能」等の要件を、分かりやすい表現で再定義すべきである。	ご指摘の箇所は、非常時の対応について示すものです。非常時に利用するアカウントは、ご指摘のようにクラウドサービス事業者の管理者、運用者等のアカウントのほか、利用者側においても、利用者側の権限管理者、エンドユーザー等、サービス内容、サービス提供形態等によりさまざまなものあり、想定される事案に応じて、適切な権限・機能を持たせることが求められます。そのため、非常時における対応の網羅性や柔軟性などを勘案すると、それぞれのアカウントに求められる権限・機能を個別に例示するよりも、一般的な記述の方が非常時対応のための要求事項として妥当であると考えておりますので、原案のとおりとさせていただきます。		
73	個人C	個人	GL	P107	3.2.8(2)(イ)4.④	ここで使われる「サーバ・ストレージ」は第2章の「インフラ」の事でしょうか？語句の統一をお願いします。	サーバ・ストレージは、インフラそれ自体ではありません(インフラにはネットワーク、データセンター施設等も含まれる）ので、原案のとおりとさせて頂きます。		
74	i医療システム機器ベンダー	法人	GL	P107	3.2.8(2)(イ)4.④	（意見） 国内法の適用が及ぶ場所の定義が曖昧と思います 加えて、クラウド事業者の事業展開によってはサービス停止のリスクもありますので、「医療機関等とのSLAや契約で国内法の適用が及ぶ場所に設置する旨を記載する」など具体的に言及したほうがよいと思います	ご指摘を踏まえて表現を修正いたします。 なお、SLA参考例で機器の設置場所を記載する項目を設けており、その項目についての考え方において、本ガイドラインの要求事項を確認しておりますので、ご指摘の趣旨は踏まえているものと認識しています。	3.2.8(2)(イ)4.④ 「③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、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する。」	3.2.8(2)(イ)3.④ 「③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、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執行が及ぶ場所に設置する。」

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
75	BSA ザ・ソフトウェア・アライアンス	法人	GL	P107	3.2.8(2)(イ)4.④	クラウドによる堅牢なデータ保護とデータローカライゼーションの問題 当社は、医療情報が機微な健康データを含み得ること、また、かかるデータに関するプライバシー保護を確実にするために、各国が適切なルールを策定する場合があることを認識しています。しかしながら、当該データを自国に保管することを命じることが、必ずしもプライバシー保護の目的達成に資する訳ではありません。クラウドサービスの大きな利点の1つである費用効率の便益を最大化するためには、グローバルな規模でデータ移転を最適に行う必要があり、円滑な越境データ移転をグローバル規模で確保することが非常に重要です。電子データのセキュリティは、データの処理又は保存をどこの場所で行うかよりも、処理及び保存を行う事業者により用いられる技術及び実践にはるかに大きく依存します。今日、主要なクラウドサービス事業者は、事業者が自ら合理的に行うことができることよりも更に堅牢なデータ保護を実施し安全管理を実践していることから、データが保存されるデータセンターの場所に拘わらず、データをローカルに保存するよりもクラウド上に保存する方が通常はより安全です。さらに、クラウドサービス事業者によっては、医療機関等を含む利用者に対して、データを保存するリージョンを選択するオプションを提供しているため、これにより、医療機関等は適用されるデータ保護及びその他のルールを遵守することがさらに容易になります。 当社の見解では、本ガイドライン中の情報および機器の所在地に関する記述は、医療機関等が日本の所管官庁に対して必要な情報を円滑に提出できるようにするという理由で、データ、アプリケーション及びハードウェアが日本に所在することを要求しているとも読むことができ、これは越境データ移転を制限する可能性があります。このような制限は、診療録に関するプライバシー保護およびセキュリティ確保という目的達成のために必要とされる制限よりも大幅に大きな制約であって、医療機関等が需要に応じて必要な情報にアクセスし提供することを可能にするために必ずしも必要なものとは言えません。さらに、そのような要求事項は、クラウドサービスの使用を利用者に思いとどまらせる可能性があります。したがって、貴省に対し、当該記述（以下の「本ガイドラインの具体的な箇所に関するコメント3をご参照下さい）を削除するよう求めます　。	ご指摘の要求事項の趣旨は、医療機関等や医療従事者における事故等が明らかになった場合に、調査機関等に対して証拠となる情報が適切に提出されることを確保するために、法定保存義務のある医療情報を取り扱うサーバ等について、国内法の執行の及ぶ範囲に設置するよう求めるものです。 国内法で保存義務が定められているにものについて、その執行が及ぶ範囲内で取り扱うよう求めることは、必要かつ適切であると認識しておりますので、原案のとおりとさせていただきます。 なお、本ガイドラインだけでなく、経済産業省ガイドラインにおいても、「医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要」である旨明示されております。		
76	BSA ザ・ソフトウェア・アライアンス	法人	GL	P107	3.2.8(2)(イ)4.④	3. 本ガイドライン本文107頁及びSLA参考例 17頁の記載 前記のとおり、主要なクラウドサービス事業者は、堅牢なデータ保護およびセキュリティを実施しており、電子データのセキュリティは、処理または保存が行われる場所よりも、データを処理及び保存するクラウドサービス事業者によって採用される技術及び実践にはるかに大きく依存します。従って、以下の文章を削除するよう強く求めます。 （ガイドライン本文 107頁） 3.2.8 災害等の非常時の対応についての安全管理対策 （イ） 災害等の非常時の対応についての安全管理対策 「④　③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、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、サーバー・ストレージ等は国内法の適用が及ぶ場所に設置する。」 （SLA参考例 17頁） 3.3 サービス提供環境・運用に係る前提条件 「乙は本サービスの提供に係る受託情報、プログラム等の保存、及びこれらに関するサーバー等の機器類は、日本国の法令の適用が及ぶ場所に設置する。」 クラウドサービス事業者のハードウェアや委託されたデータを日本国内に留めることを要求する必要はありません。医療機関等は、データおよびサーバー等がどこに存在するかにかかわらず、契約によって、リアルタイムにデータにアクセスして、所管官庁に必要な情報を円滑に提供することを確実にすることができます。	ご指摘の要求事項の趣旨は、医療機関等や医療従事者における事故等が明らかになった場合に、調査機関等に対して証拠となる情報が適切に提出されることを確保するために、法定保存義務のある医療情報を取り扱うサーバ等について、国内法の執行の及ぶ範囲に設置するよう求めるものです。 国内法で保存義務が定められているにものについて、その執行が及ぶ範囲内で取り扱うよう求めることは、必要かつ適切であると認識しておりますので、原案のとおりとさせていただきます。 なお、本ガイドラインだけでなく、経済産業省ガイドラインにおいても、「医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要」である旨明示されております。		
77	HEASNET	法人	GL	P115	3.2.9(2)(イ)2.	(ア)ネットワーク経路に関する安全管理対策の項目に記載すべきと考えられる。	ご指摘を踏まえて修正いたします。	3.2.9(2) (ア) ネットワーク経路に関する安全管理対策 1.ネットワーク経路における安全管理対策 2.医療機関等からの経路の確認 3.ネットワーク経路対応に用いる機器 (イ) ネットワーク経路以外の通信上の安全管理対策 1.暗号化対策 2.通信経路の暗号化対策 3.回線の品質等 4.仮想デスクトップ (ウ) 保守における通信上の安全管理対策	3.2.9(2) (ア)ネットワークに関する安全管理対策 1.ネットワーク経路における全般的な安全管理対策 2.医療機関等からのネットワーク経路の確認 3.ネットワーク経路対応に用いる機器 4.暗号化対策 5.通信経路の暗号化対策 6.回線の品質等 7.医療機関等の外部からのサービス利用 （削除） (イ) 保守における通信上の安全管理対策
78	帝人ファーマ㈱	法人	GL	P115	3.2.9(2)(イ)2.②	■意見の概要 ・『SSL-VPNは原則として使用しない』の記載を、『SSL-VPNは、クライアント型を除いて、原則として使用しない』に変更したほうが好ましい。 ■意見および理由 ・近年、外部検査機関からの検査結果や、医療機器の遠隔データ通信に、安全・低コスト・汎用性の高い通信方法が求められており、その中でSSL-VPNも有効な手段である。 ・本ガイドラインが参照している、SSL/TLS暗号設定ガイドラインver2.0　66ページには、下記のように記載されている。 ・『SSL-VPNには、大きく3通りあり、クライアントレス型、on-demandインストール型は、本質的にはSSL/TLSと同じものとみられ、クライアント型はモバイル型のIPsec-VPNに近い運用形態となる。』 ・『クライアント型SSL-VPNは、誤って偽サーバに接続することがなく、また内部サーバにアクセスできる端末も厳格に制限できる。機密度の高い情報を扱うのだとすれば、少なくともクライアント型でのSSL-VPNを利用すべきである。』 ・技術的観点からも、クライアント型SSL-VPNでは、経路を暗号化する過程で盗聴されるリスク、偽サーバへ接続するリスク、セッション間の回り込みによる攻撃のリスクの対策が可能である。	ご指摘の要求事項は、厚生労働省ガイドラインで、「いわゆる 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」とされていることを踏まえて定めており、原案の通りとさせて頂きます。		
79	株式会社ビーグル	法人	GL	P121	3.2.10(2)(ア)	治験業務で医師に電子証明を依頼することがございます。３．２．１０法令で定められた・・・には電子証明書を用いて電子署名を施すとあり、電子証明書の取得が必須のように取れましたが、治験にかかわる全医師に電子証明書を取得頂くのは難しいと考えます。そのため、広い意味での電子署名を行う際には、アー2記載の確認をすることで、良いということでしょうか。	ご指摘の要求事項は、法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合の要求事項でありますので、ご懸念は当たらないと考えております。		

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
80	個人G	個人	GL	P121	3.2.10(2)(ア)①	■ 3.2 医療情報サービスに求められる安全管理に関する要求事項 > 法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名に対して、保健医療福祉分野 PKI 認証局の発行する電子署名へ対応することの可否を、医療機関等に対して明らかにする ＊ 法令で定められた記名・押印を電子署名で行うものとされた情報、とは何かを明確にして頂ければと思います ＊ HPKI技術が世の中に浸透していない中で(Windows環境が前提となっているなど)、HPKI電子署名に対応すること自体が困難な状況にあります。これへの対応も合わせて検討頂ければと思います	ご指摘のうち、「法令で定められた記名・押印を電子署名で行うものとされた情報」とは、法令で署名又は記名・押印が義務付けられた文書のうち、e-文書法省令に基づいて、記名・押印に代わって電子署名を施すこととした情報を指しています。ご指摘のようなご質問があったことを踏まえ、表現を修正いたします。 一方で、ご指摘のうち、「保健医療分野PKI認証局が発行する電子署名へ対応することの可否を明らかにする」ことについては、厚生労働省ガイドラインが、保健医療分野PKI認証局が発行する電子署名を推奨していることに鑑み、少なくとも医療情報を受託するクラウドサービス事業者は、医療機関等に対して対応の可否を明らかにする必要があるため、原案のとおりとさせていただきます。	3.2.10(2)(ア)① 「法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名に対して、保健医療福祉分野 PKI 認証局の発行する電子署名へ対応することの可否を、医療機関等に対して明らかにする。」	3.2.10(2)(ア)① 「法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合に、保健医療福祉分野PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。」
81	HEASNET	法人	GL	P144	3.3.6(2)(ウ)2.③	「③医療機関等の指示に基づき、受託する医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように、3．2．3及び3．2．9に示す対応策を講じる。」 3．2．3及び3．2．9に加え、人的安全対策である3．2．4の対応策も対象と考えられる。	3.2.4に示す安全管理対策は継続的かつ包括的なものであり、特定の場合について対策を講じるよう再確認する必要はないと考えられますので、原案のとおりとさせていただきます。		
82	個人C	個人	GL	P147	3.3.7(2)(ア)①	（意見） 個人情報保護法上の「外国にある第三者への提供」が本ガイドラインにどのように反映されているのか？例えば海外にサーバがあるクラウドを活用する場合には、そのクラウド事業者が個人情報を取り扱わないという体になっていない以上、当該クラウドを利用する方（医療機関または個人情報取扱受託事業者）からの個人に対する同意が必要であることという理解で良いか？	個人情報保護法上の第三者提供に当たる場合には、個人情報取扱事業者（医療機関等）が個人情報保護法上必要な対応を行うことが求められますが、本要求事項はクラウドサービス事業者と医療機関等の間で個人情報保護対応策を合意するように求めるものでありますので、原案のとおりとさせていただきます。		
83	個人G	個人	GL	P150	3.4.1(2)①	■ 3.4 クラウドサービスの利用終了に関する要求事項 > サービス一部又は全部の停止、変更の場合(軽微なバージョンアップは含まない)には、既に提供しているサービスを利用している医療機関等への影響を最小 とするための措置を講じるほか、医療機関等が対応するのに十分な期間をもって、サービスの一部又は全部の停止、変更等に関する告知を行う。 ＊ クラウドサービスである以上全体最適な改善を繰り返すものであり、その中でこのような文言があると、各医療機関への影響を考慮しクラウドサービス全体のユーザビリティが改善しずらい状況になってしまいます。「変更の場合には」という文言の言い回しを修正するか、削除頂ければと思います	医療機関等が取り扱う医療情報は、高い可用性が求められるものであって、本ガイドラインでも可用性に関する多くの要求事項を求めていることに鑑みると、サービスを変更するに当たって医療機関等に与える影響を最小にするための措置を講じることや、医療機関等が対応するのに十分な期間をもって告知することは最低限必要な事項であり、過大な要求事項とはいえないことから、原案のとおりとさせていただきます。		
84	個人G	個人	GL	P151	3.5.2②	■ 3.5 オンライン診療システム提供事業者における安全管理対策 > オンライン診療システムに用いられるクラウドサービスにおいて、患者側端末で利用されるオンライン診療システムの機能に、オンライン診療の実施中に医療 情報システムと接続する機能等を含まないこと、及びこれに関する情報提供につ いて、オンライン診療システムを提供するクラウドサービス事業者は、サービス仕様適合開示書に基づき、医療機関等と合意する。 ＊ オンライン診療に関する要求に関しては「オンライン診療の適切な実施に関する指針」にて整理されている中で、再度本ガイドラインに組み込む背景は何でしょうか。個別オンライン診療に関する記述は削除し、本ガイドラインではクラウドサービス事業という大枠で整理して頂ければと思います	ご指摘の「オンライン診療の適切な実施に関する指針」は、オンライン診療システムと医療情報システムの接続がある場合について、本ガイドラインを含む医療情報安全管理関連ガイドラインに沿った対策を行うよう求めています。 それを受けて、本ガイドラインにおいて、医療情報システムと接続があるオンライン診療システムを提供するクラウドサービス事業者に対する具体的な要求事項を整理したものでありますので、原案のとおりとさせていただきます。		
85	MITSF（メディカルITセキュリティフォーラム）	法人	GL	PP152-172	3.6全般	【PHRサービス事業者の努力義務の根拠について】 3．6．1「PHRサービス事業者への要求事項」では、"医療機関等での医療情報の利用とPHRでの医療情報の利用を比較した際に、医療情報の機密性に変化は無い"と記載される。 一方、3．6．4「PHRサービス事業者の努力義務とする要求事項」では、患者本人が事業者を選択しているのだから、PHRサービス事業者にも医療データ（PHRデータ）の機密性への対策は努力義務で良いとされており、主旨が相反しているように見受けられる。 そもそも、完全性や可用性がそれほどもとめられないのがPHR事業者という記載からも、努力義務は完全性や可用性の面で課されはしても、機密性においても斟酌すべきものなのか。 そのため、患者が自発的に選択したPHRサービス事業者には、医療情報の機密性に変化がないにも関わらず、3．2．3のア-（4）-③、カ-1-⑤を必須事項として遵守しなくてよい根拠をもっと明確に、丁寧に提示すべきである。 PHR事業者は要配慮個人情報の取扱いは雑でも良いとガイドラインが認めたように読めてしまうことが懸念される。 （本ガイドラインがそのように意図しているのであれば、その点をもっと明確化すべきである） なお、機密情報を取り扱う、医療業以外の一般の情報処理事業者は、今日、NISC主管の業界セプターやISAC組織等でカ-1-⑤のような対策は当然のように求められるにもかかわらず、PHR事業者のみが優遇される理由も不明確である。 業界横断的なセキュリティ標準の観点より、PHR事業者には脅威情報の収集・管理（カ-1-⑤）を実施することを努力義務に留める理由も明確化していただきたい。	ご指摘のようなご懸念を踏まえ、ご指摘の項目について、所要の修正や読替えを実施した上で、3.6.2のPHRサービス事業を適用対象とする要求事項として整理し、3.6.4のPHRサービス事業者の努力義務とする要求事項は設けないこととさいたします。	3.2.3(2)(カ)1.⑤ 「システムの脆弱性に関する情報をJPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティ センター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源に、日次及び必要なタイミングで確認する。」 3.6.1 （挿入） 「⑤ PHRサービス事業者については、3．2．1～3．2．9、3．3．6～3．3．7に示す要求事項のうち、3．6．4に掲げる項目については、上記①による読み替え後の要求事項を努力義務とする。」 3.6.4	3.2.3(2)(カ)1.⑤ 「情報システムの脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。」 3.6.1 「③ PHRサービス事業者については、3．2．3（2）（ア）4.の③の要求事項における「なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第5版の公表（平成29年5月）から約10年後を目途に2要素認証について「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。」とある部分を削除するものとする。」 （削除） （削除）
86	個人G	個人	GL	P153	3.6.1⑥	■ 3.6 PHR サービス事業者における安全管理対策 > PHR サービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。 > ・登録時の ID 申請者である患者等の本人確認(実在性の確認) > ・利用時の患者等の認証(利用者の本人確認) > ・医療機関等が管理していた患者等の医療情報と、利用する患者等の ID との紐づけ(患者本人の情報であることの正確性) ＊ PHRサービスの定義をより厳密にするべきであると考えます。例えば、身長/体重/血圧などを管理するだけのクラウドサービス（アプリ）に対してもこのような水準を求める必要があるのでしょうか。そのような簡易アプリに対しても本人確認を行うことで、より個人情報漏洩のリスクを増加させるものになり得ると考えます ＊ また医療機関の管理している医療情報と患者IDの紐付けの実際のオペレーションが不透明である以上、「医療機関等が管理していた患者等の医療情報と、利用する患者等の ID との紐づけ」という記述は不要なのではと考えます	本ガイドラインは、「クラウドサービス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」であって、PHRサービス事業者について、「PHRサービスを提供するクラウドサービス事業者。医療情報の取扱いを目的としないクラウドサービス事業者は、本ガイドラインにおけるPHRサービス事業者には該当しない。」と定義しておりますので、ご指摘のようなご懸念は当たらないと考えております。 また、ご指摘の「医療機関等が管理していた患者等の医療情報と、利用する患者等の ID との紐づけ」の手順を定めることを求める事項は、PHRサービス事業者が、患者等や医療機関等から新たに情報を受領した場合に、患者本人の情報であることを確認して、登録されている患者等のIDと紐付けるための手順を定めるよう求めるものであり、PHRサービスを実施する上で必要なものであるため、その趣旨を明らかにするよう表現を修正した上で、要求事項としては維持させていただきます。	3.6.1⑥ 「PHRサービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。 ・登録時のID申請者である患者等の本人確認(実在性の確認) ・利用時の患者等の認証(利用者の本人確認) ・医療機関等が管理していた患者等の医療情報と、利用する患者等のIDとの紐づけ（患者本人の情報であることの正確性）」	3.6.1⑥ 「PHRサービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。 ・登録時のID申請者である患者等の本人確認（実在性の確認） ・利用時の患者等の認証（利用者の本人確認） ・新たに受領した医療情報の患者等のIDへの紐づけ（患者本人の情報であることの確認）」

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
87	一般社団法人日本画像医療システム工業会	法人	GL	P173	第4章	意見：“「対策済み」であることが期待されている。”が本体の主旨においては「対策済み」に出来ない場合、厚生労働省ガイドラインに基づき、医療機関への説明義務及び合意形成が必要である旨の説明まで記述すべき。 提案する記述文：例えば以下のような表記にする。 “「対策済み」であることが期待されている。医療機関が満たすべき厚生労働省ガイドラインに対して未達内容がある場合、そのことと追加対策を医療機関側に明示し、十分協議の上対応する必要がある。”	本ガイドラインへの適合状況については、医療機関等に対してサービス仕様適合開示書を提示するスキームとしておりますので、提供するサービスの特性によって対象外となる項目についても、同開示書で提示いただくことを想定しております。		
88	個人A	個人	GL	P173	4.1.1	p173に記載の内容について疑義があるため訂正を求める。 「契約、SLA 等による対応の必要性」にて「また、提供するサービスレベルが提供コストに大きく影響する安全管理上の対応については、 業務要求とコストのバランスにおいて適切なサービスレベルを両者で合意することが求められる。」 とあるが、コストを削減するためにSLAや情報セキュリティのレベルを下げることを許容していると感じた。 事業者にとってみれば情報セキュリティはコストである。よって価格競争による情報セキュリティの低下が懸念される。 情報は流出すればそれを削除することは実質的に不可能であり、この被害を受けるのは患者である。	当該記載は、医療機関等がクラウドサービスの利用コストを下げるために、クラウドサービス事業者との適切な役割分担の中で、安全管理対策の一部を医療機関等自ら実施する場合を想定したものであり、情報セキュリティレベルの低下を許容するものではありません。 ご指摘のようなご懸念が生じないよう、ご指摘を踏まえて修正いたします。	4.1.1 また、提供するサービスレベルが提供コストに大きく影響する安全管理上の対応については、業務要求とコストのバランスにおいて適切なサービスレベルを両者で合意することが求められる。	（削除）
89	HEASNET	法人	GL	P174	4.1.2	誤記 ～コミュニケーションが参考になる。表33に示すように～ 【修正後】 ～コミュニケーションが参考になる。表3に示すように～	ご指摘のとおり、表記の誤りのため、修正いたします。	4.1.2 「表 33に示すように、製造業者は、製品に係るセキュリティ情報を提供するにあたり、標準化された書式を用いることで一律に利用者に対して情報提供を行っている。」	4.1 「医療情報システム機器では下の＜「製造業者による医療情報セキュリティ開示書」の目的＞に示すように、製造業者は標準化された書式を用いることで製品に係るセキュリティ情報を一律に医療機関等に提供している。これにより医療機関等は、製造事業者におけるセキュリティ情報の比較やレビュー、ガイドラインへの適合状況の確認を容易に行い、機器等の選定を行うことができる。」
90	JAHIS	法人	GL	P174	4.1.2脚注33	最新版としてVer.3.0aが制定されていますので、そちらへのポイントをお願いします。	ご指摘を踏まえて修正いたします。	4.1.2脚注33 「JAHIS「製造業者による医療情報セキュリティ開示書」ガイドVer.2.0（2014年11月　一般社団法人 保健医療福祉情報システム工業会医療情報システム部会 セキュリティ委員会開示説明書WG）」	4.1脚注39 「JAHIS「「製造業者による医療情報セキュリティ開示書」ガイドVer.3.0a」（2017年7月　一般社団法人 保健医療福祉情報システム工業会医療情報システム部会 セキュリティ委員会 開示説明書WG）、JESRA TR-0039*B「「製造業者による医療情報セキュリティ開示説明書」ガイド Ver.3.0a」（2018年1月　一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会JIRA-JAHIS合同開示説明書WG）」
91	一般社団法人日本画像医療システム工業会	法人	GL	P174	4.1.1脚注33	意見：「製造業者による医療情報セキュリティ開示説明書」ガイド」 はJIRAからも発行しており併記が必要 提案する記述文：以下を併記する。JESRA TR-0039*B「「製造業者による医療情報セキュリティ開示説明書」ガイド Ver.3.0a」一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会JIRA- JAHIS合同開示説明書WG	ご指摘を踏まえて修正いたします。	4.1.2脚注33 「JAHIS「製造業者による医療情報セキュリティ開示書」ガイドVer.2.0（2014年11月　一般社団法人 保健医療福祉情報システム工業会医療情報システム部会 セキュリティ委員会開示説明書WG）」	4.1脚注39 「JAHIS「「製造業者による医療情報セキュリティ開示書」ガイドVer.3.0a」（2017年7月　一般社団法人 保健医療福祉情報システム工業会医療情報システム部会 セキュリティ委員会 開示説明書WG）、JESRA TR-0039*B「「製造業者による医療情報セキュリティ開示説明書」ガイド Ver.3.0a」（2018年1月　一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会JIRA-JAHIS合同開示説明書WG）」
92	個人C	個人	GL	P176	4.2	本文「・・・、具体的に第3章でサービス仕様適合開示書によって提示すべきものとしたものを以下に示す。」 若干日本語がおかしいと思われます。「・・・提示すべき要求項目を以下に示す。」などの表現ではどうでしょうか	趣旨を明確にするため、ご指摘の箇所の表現を修正いたします。	4.2 「ここでは、4．1．2で示したサービス仕様適合開示書を通じた合意形成をすることを想定し、具体的に第3章でサービス仕様適合開示書によって提示すべきものとして示したものを以下に示す。」	4.2 「ここでは、第3章に示した要求事項のうち、サービス仕様適合開示書により情報提供すべき項目を示す。」
93	個人G	個人	GL	P178	4.2(6)	■ 4.2 合意形成を行なう内容 > 標準形式を採用していない項目の場合のデータ項目の形式、標準形式への変換等への対応 * 例えば診療録データの標準化フォーマットに対する仕様や指針が不透明であるため(HL7/CDAが標準化フォーマットなのか否か)、標準化フォーマットの明確化と出力のための技術サポートなども合わせて対応頂ければと思います	ご指摘の「標準化フォーマットの明確化と出力のための技術サポート」については、本ガイドラインで規定すべき範囲を超えているため、本ガイドラインで対応することは困難ですが、今後の施策検討に当たって参考にさせていただきます。		

NO.	氏名・名称	属性	資料	ページ（原案）	パート（原案）	意見	方針・コメント	修正内容	
								原案	修正後
94	MITSF（メディカルITセキュリティフォーラム）	法人	GL	その他	その他	【GDPR等海外のデータ規制について】 2015年12月、EU当局から一般データ保護規則(General Data Protection Regulation: GDPR)が公開され、2016年4月に採択された後、2018年5月25日から適用されている。 GDPRの観点から、クラウドサービス事業者は「処理者」の位置付けになるが、仮に医療機関がEU居住者の患者データを取り扱い、その処理をクラウド事業者に外部委託している場合、GDPRの第3条（域外移転の原則）、第28条・29条（外部委託先適用）の観点より、クラウド事業者はGDPRに基づくデータ管理体制を整備することが求められる。 例えば、電子カルテサービスを提供するクラウド事業者に外部委託を行う日本の医療機関において、EU居住者が当該医療機関で受診し、そのカルテ情報（個人データ）を外部委託先がクラウドサービスにて処理する場合、外部委託先であるクラウド事業者にもGDPR遵守が求められることが考えられる。 また、EU居住者で、日本に短期滞在する外国人医師も含め、院内の人事データを日本のクラウドサービス事業者へ委託している場合、当該事業者もGDPRを遵守することが原則的には求められる。 今回のガイドライン改定には、このような海外のプライバシーデータ規制への対応を定めることが目的でないとしても、このような観点がガイドラインのどこにも記載されないことにより、日本のクラウド事業者をミスリーディングするリスクがある。 そのため、GDPRに代表される、海外のデータプライバシー規制に関する注意文、つまり、日本の個人情報保護法やe-文書法省令、外部保存通知等を準拠することと同時に、取り扱われる患者データに海外関係者が含まれる場合には、海外の法規制への配慮をしなければならない点は明確に啓発すべきである。 例えば、GDPRのみではなく、中国のインターネット安全法もGDPRに近い観点で見直しが行われようとしている。インバウンド型の健診サービス等を提供する日本の医療機関等が利活用する、日本の外部事業者のデータ管理ガバナンスは極めて重要と思われる。	本ガイドラインでは、医療機関等との契約において、関連法令を遵守する旨を明らかにするよう要求事項に含めております。(3.2.1(2)(イ)2.①)。ここでいう法令は、提供するクラウドサービスに適用される法令全般を指すため、仮に海外の法令が適用される場合には、当然にその法令も含まれます。 海外の法令は多数存在するため、そのうちの1つについて特記することは適当ではないと考えておりますが、ご指摘があったことを踏まえ、上記の趣旨を明らかにするために、必要な修正をいたします。	3.2.1(2)(イ)2.① 「サービス提供に係る契約において、次項（ウ）1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。」	3.2.1(2)(イ)2.① 「サービス提供に係る契約において、次項（ウ）1.に定める運用管理規程等の内容、その他最新の関連法令等（注）を遵守し、安全管理措置を実施する旨を明らかにする。」 （注）当該サービスに関係する日本国外の法令を含む。
95	個人H	個人	GL	全般	全般	医療情報であることを前提とした立て付けであり医療情報基点のPHR、PHRサービスのみが対象となっているが、PHRサービスには個人基点も含まれるはずであり、PHRサービス全体を網羅したガイドライン、ルール作りが求められるのではないか？ ・医療情報＝医療機関で収集・作成された情報が出発点となっているため、個人が集める健康情報が網羅されない ・P12　に管理主体が個人に移ったところからPHRとの記載があるが、PHRには医療情報に含まれない、例えば日々の活動量、食事や睡眠の記録なども含まれるはず ・「医療情報の取扱いを目的としないクラウドサービス事業者は、本ガイドラインにおけるPHRサービス事業者には該当しない。」とあるが、医療情報を取り扱わないPHR事業者が参考にするガイドラインがない。 ・国際標準化機構（ISO）から発信されているテクニカルレポートISO/TR 14292におけるPHRの定義は「情報管理の一切の権限をデータの主体である個人が持つ健康関連情報」、とされている。医療情報だけに限らず、日々の生活情報なども含んだ広い意味を持つ言葉としてPHRを広げる必要があるのではないか。 ・本ガイドラインが先行することで、全てのPHRサービス事業者が、医療情報を基点としたPHRを想定した本ガイドラインを遵守しなければいけないとの誤解が広がる懸念がある。	ご指摘を踏まえて、趣旨が明らかになるように修正させていただきます。 なお、本ガイドラインは、クラウドサービス事業者における医療情報の安全な取扱いを確保することを目的として、いわゆるPHRサービスを提供する事業者のうち医療情報を取り扱う事業者を対象として要求事項を整理したものです。そのため、いわゆるPHRサービス事業者全般に対するガイドラインを策定すべきといったご意見については、今後の検討の参考にさせていただきます。	1.2.2 PHR 「患者等が医療情報を自らの判断のもとで活用する仕組み。」	1.2.3 PHR 「個人の生涯にわたる医療・健康等に関するデータを時系列で管理し、本人の判断のもと多目的に活用する仕組み。PHRは、広く個人の健康に関連する様々な情報を活用する仕組みを指すが、本ガイドラインにおけるPHRは、医療情報を活用する場合を対象とする。」
96	個人H	個人	GL	全般	全般	個人を主な契約対象としたPHRサービス事業者への要求事項について ・（ガイドラインの対象が医療情報基点のPHRサービスという前提のため）医療情報の特殊性、高度な安全性の要求という点が強調され過ぎて、PHRサービスの展開、利用の促進の障壁となりかねないのではないか？ ・PHR＝管理主体が個人に移った後の安全管理の指針がP152以降に記載されている。注釈で、「ただし、PHRサービスの場合、医療機関等が医療情報を取り扱うクラウドサービスを利用する場合と異なり、患者等が取り扱う医療情報は自らの情報に限られることから、PHRサービス事業者における要求事項への対応は、それに応じた水準・内容となる。」とあるが、要求事項が多すぎるように感じる。個人主体のPHRの場合は、医療機関等が団体として医療情報を管理する場合とは異なり、コストベネフィットを元に個々人が自由にサービスを選び活用する権利を有するはず。要求が多いほどサービス提供にコストがかさむことになるため、結果として個人の自由なサービス利活用を損なう恐れがある。要求事項はユーザー個人の重篤なリスクを回避する範囲に限定すべきではないか。 ・152ページ以降、図14等に示される主たる契約相手が「個人」であるPHRサービス事業者については、本ガイドラインの要求範囲には含めずに、前述の通り医療情報以外も含むより広い範囲を包括したPHRサービスガイドラインの中で規定するべきではないか。	医療情報については、その管理が患者等に移ったものであっても、その漏洩や改ざんによって、個人の権利が侵害されたり、適切な医療を受けられなくなるといったおそれがあるため、そのリスクを低減させるために原案に掲げた要求事項を遵守いただくことが必要であると認識しておりますので、原案のとおりとさせていただきます。 なお、いわゆるPHRサービス事業者全般に対するガイドラインを策定すべきといったご意見については、今後の参考にさせていただきます。		