医療情報システムの安全管理に関するガイドライン第 5.1 版（案）　パブリックコメント意見　（別紙）

整理番号	章	意見	考え方	修正内容	
				原案	修正案
1	全般	第 6 章において、守秘義務が法的に保証され、技術の維持・研鑽が更新の条件となっている、情報セキュリティに関する国家資格である情報処理安全確保支援士の関与を求めることにより、挙げられている課題の解決がより効率的かつ正確に行えると考えられる。 6.5 の技術的安全対策の検討に関し、情報処理安全確保支援士の関与を求める事により、専門家としての知見を活かした対応の提案が期待できる。 よって、推奨されるガイドラインに、関与を求める事を挙げることを提案する。 6.6 の人的安全対策については、まさに情報処理安全確保支援士が、医療情報システム安全管理責任者に適任であると考える。 情報処理の促進に関する法律に定められている通り、情報処理安全確保支援士には守秘義務が課せられており、また、欠格事項も存在するため、信頼に値する人材と言うことができる。 さらに、インシデント発生時のインシデント取り扱いや情報の安全管理に関する教育訓練は、情報処理安全確保支援士の業務であるため、適格だと考える。 推奨されるガイドラインに、医療情報システム安全管理責任者も求める資格として、情報処理安全確保支援士を挙げることを提案する。	参考意見として承りました。		
2	6	「6. 医療情報システムの基本的な安全管理」に記載の「医療情報システム安全管理責任者」について、特に第 6 章では ISMS についても言及していることから、これに精通していることが認定されている国家資格である「情報処理案件確保支援士」の活用に言及することが望ましいと考えます。	参考意見として承りました。		
3	全般	パスワードを使用する場合の要件に 「英数字、記号を混在させた」との複雑性を強要する文言が入っています。NIST が方針転換したのはパスワードの定期変更だけでなく、パスワードの使いまわしを防ぐため、パスワードの複雑性を強要しない　という点についても見直しされています。 もう 3 章 2 ガイドラインに統合されましたが、総務省のガイドラインでも強要のない表現にうまく訂正されていました。 パスワードの使いまわしを防ぐためにも、「英数字、記号を混在させた」という表記を消すか、ユーザーにパスワード強度を意識させて　ユーザーが設定したいパスワードを阻害しないような条件にすべきではないでしょうか。	NIST600-63-3 では 5.1.1 において「Verifier は他の構成ルール(例えば，異なる文字種の組み合わせ，一定の文字の繰り返し)を記憶シークレットに課すべきではない」とされていおり、同付録Aの「A.3　複雑さ」においては、例えば「大文字と数字を含む要件を与えると，比較的高い確率で”Password1”を選択し，記号を要件に追加すると”Password1!”を選択する．」という例が示されています。しかし NIST の指摘の趣旨は、「容易に推認できる PW]の設定につながるのであれば、複雑性を求めるのは妥当ではないとすることであり、本ガイドラインでは、元々、容易に推認可能な PW 設定は行わないようにする、としておる前提があります。その中でさらに複雑性を設けている構造としており、複雑性だけを要件として、結果として推認可能な PW を許容するものではありません。これらを勘案して、原案のままとさせていただきます。		
4	8.1.3	125 頁の個人情報保護についての現状との相違と問題点 医療情報という極めて機微な個人情報を医療関係者が閲覧できる事について。 町医者では効率を重視して、診察の時に医師の他に複数の地域採用のパート看護師が補助についており、会話の内容も必然的に耳に入る。また、病院の受付でレセプト入力も同じく地域採用のパートで、その人達には守秘義務があるというが、特に厳格な教育や指導はなく、現状では業務必要以外の患者さんの個人情報を話している姿をよく目にする。 薬局においても、同じようにパートの受付の人が処方箋を入力する権限を持ち、仕事の合間にはそこ	参考意見として承りました。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		から得た患者の話をしている。また日常的にパートが薬の仕分けの補助をやっている姿もよく見かける。 以上のような事から、今の医療体制のまま、情報を閲覧できる権限が広範囲の人間が持てれば、簡単に個人の医療情報が地域採用のパートさん含め外部に漏れている。また、個人がどんな病気を持っているか、薬を服用しているかも、医療関係者であれば、複数の人が簡単に一目でわかり、そうした情報が雑談から地域に漏れる可能性が考えられる。 今後、過去の病歴や薬歴、カルテ情報がマイナンバーカードを活用する事により、本人同意があれば、どこの病院、薬局でも簡単にわかってしまう事で、更に今まで以上に、個人が知られたくない病気や過去の薬歴、カルテ情報が地域採用の人達から漏れる事が予測され、個人が地域で生活しづらい環境が生まれる事が危惧される。 こうした新制度を実行する前に、医療現場で働く人達の守秘義務の再教育や、医療情報を閲覧できる人を限定する法律の制定、個人情報が不本意に漏れたりしないよう、また漏れた場合に国民が相談できる、第三者機関を国が自治体ごとに設置し、監督、指導、相談業務をさせる必要性があると考える。 さらに、学校健診等の情報も、過去に遡り、紐付けするとの事だが、不登校や心の病気などを経験した子供が多い世の中、そうした過去の事を学校健診の記録に記載されることにより、将来の進学や就職する時の健診時において不利益を被る事がないように十分配慮する必要がある。 (就職時の健診時の医師のコメント一つで過去の忘れたい病歴や薬歴が問題視され、本人が知らないところで不利益を被る事がないようにして欲しい) また、大人でも不妊治療や流産、心の病気やその他、個人が知られたくない病気や過去の病歴、薬歴などがあることを考慮してほしい。(緊急事態時を除く)例えば、現状のままカルテが共有化された場合、歯医者に行っても過去に不妊治療や流産していた事が医師、受付、看護師にわかる。こうした仕組みを変えてほしい。 また、本人が医療情報の閲覧を同意しなければ、医師や薬剤師が情報を閲覧する事ができなくなるが、その事について患者に詰問するなど圧力をかけたり、同意がないにも関わらず、医師や薬剤師の権限で勝手に閲覧することを禁止する条文を加えてほしい。 さらに、医師や薬剤師は必ずしも皆、人格者とは限りらない。カルテ情報にも事実だけでなく、患者との会話内容から一部を抜粋したプライベートな記録や、診察した医師の個人的価主観、価値観もコメントとしてカルテには記録に残されている。 一方、患者は余程の事がない限り、カルテ情報を見ることはできない為、今後、医師同士での情報共有が可能になった場合、そうした点についてそれぞれの医師が情報を、全て鵜呑みにする事がないよう、患者を色眼鏡で見ることがないよう、国がカルテ情報のどこまでを共有するのか精査し、医師にもガイドラインを作成し、指導する必要があると考える。 また、薬剤師においても、医師と同等のレベルで、患者に対して、症状を事細かに聞いて、薬剤カルテに情報を色々入力している現状がある。ここでも薬剤師個人の主観や価値観の入ったコメントが予測されるので、それを医師や他局の薬剤師が見て、患者に先入観や不利益がないよう、国が薬剤指導カルテのどの情報までを共有するのか、国が精査し、薬剤師向けにもガイドラインを作成し、指導、教育する必要があると考える。 また、医療関係者(パートや契約社員含む)に患者の個人情報保護の教育の徹底、もし、個人情報が漏れた場合の罰則規定をもっと厳格し、第三者機関がこれらを監督し、パートや契約社員にも適用して欲しい。 また、患者側も個人情報が漏れる可能性が不安な時は、その第三者機関に気軽に相談できるような体制を作ってほしい。			

整理番号	章	意見	考え方	修正内容	
				原案	修正案
5	6.10	6.10(4)非常時に備えたセキュリティ体制の整備で言及された”一定規模以上”の病院や、”地域で重要な機能を果たしている医療機関等”の基準が不明瞭であり、対象となる医療機関が厚労省によりなんらかの基準が示されるか、或いは病院機能や床数を示す等により、明確な線引が必要と考えます。同じく情報セキュリティ責任者、CSIRT 人員には一定の技術レベルが必要であると同時に、セキュリティ体制の構築も病院規模等により最適な形態が異なると考えます。また医療機関等においては、そうした役割を担うことができる高度情報人材は非常に限定的と思われ、形骸化した目標と化し、緊急時の対応ができないといったケースが散見される状況がみられることも想定されます。人材育成、技術レベル確保の観点からも、特に対象の医療機関は明確化し、診療報酬点数表へ加算として継続的に支援、重視することを明確化いただくことが全国的な体制の整備に資するものであると考えます。	ご指摘いただいた箇所においては、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等」の役割やリスクに鑑みて、非常時のセキュリティ体制について定めたものですが、機能やリスクは具体的に医療機関等が果たしている役割や所在する地域によって異なることから、一律に基準を示すことは、却って適切な体制をつくりにくくなる可能性が生じ、本項の趣旨に合致しない結果が生じうるところです。このような観点から原案の通りとさせていただきます。		
6	6.11	P86: 無害化についての確認。 外部から取り込むデータの無害化の表記では内容が不明確。 製品により無害化、無効化など表記が異なるものがある。 単に該当するオブジェクトを削除し動作を無効にする製品などがある。 今回の医療データを取り扱うに辺り、データの改変など、医療ミスにつながるような処理は無いなのか、法令に照らし合わせて問題のない無害化の定義と内容を明確に解説していただきたい。	本ガイドラインが想定している「無害化」につきましては、用語集で内容を定義しました。		
7	6.8 8.1.2	意見1： 8.1.2 c2.(9)e にはいわゆる ISMS クラウドセキュリティ認証（JIP-ISMS517）は記載されていませんが、「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」には認証制度として冒頭に「ISO/IEC 27017 による認証取得」が記載されています。この制度は国内医療業界でも比較的馴染みのある制度です。 いわゆる ISMS クラウドセキュリティ認証（JIP-ISMS517）の認証を取得したサービス（事業者）は、8.1.2 c2.(9)e を満たすかどうかについて、Q＆A集でもよいので明確にしていただきたい。	ご指摘を踏まえて、JIS Q 27001、JIS Q 15001 について、8.1.2 c2.(9)e として確認内容として追記し、従来の 8.1.2 c2.(9)e は示し、従来の 8.1.2 c2.(9)f として項番を繰り下げました。その他の認証等につきましては、具体的な内容を QA に記載し、その中に反映しました。	d 財務諸表等に基づく経営の健全性 e 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 ・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7 号） ・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 f 医療情報を保存する機器が設置されている場所(地域、国) g 受託事業者に対する国外法の適用可能性	d 財務諸表等に基づく経営の健全性 e JIS 15001、JIS Q 27001 の認証の有無 f 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 ・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7 号） ・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 g 医療情報を保存する機器が設置されている場所(地域、国) h 受託事業者に対する国外法の適用可能性
8	6.8 8.1.2	意見2： 8.1.2 c2.(9)e にいわゆる ISMS クラウドセキュリティ認証（JIP-ISMS517）を含めると仮定した場合、一般的にサービスイン後、一定の期間を経ないと認証を取得できないし、認証取得を急ぎ過ぎれば実力を伴わない形骸的な認証取得になると思います。サービスインから認証取得までの期間はどの程度許容されるのか、考え方又は基準を示すべきと思います。	8.1.2 c2.(9)e については、医療機関等が委託先事業者を選定する際に、確認すべき事項であり、本ガイドラインでは、その有無を委託の要件としているわけではありません。医療機関等が扱う情報管理状況等に応じて、医療機関等が必要に応じて求める		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
			べき内容として確認する項目を示す趣旨ですので、ご指摘のような考え方等は、個々の医療機関等が確認に際して、事業者に対して具体的に求めるものであると解しております。よって原案のままとさせて頂きます。		
9	6.8 8.1.2	意見3： 6.8c.2.に有った「保守要員個人の専用アカウント」が「保守要員の専用アカウント」に変更されています。この背景にある考え方をQ＆A集などでもよいので解説頂きたい。	今回の表現の修正については、保守要員ごとに専用アカウントを付与することを想定しているものでありますが、そのアカウント自体が個人に必ず紐づかなければいけないという趣旨ではありません（A というアカウントを甲が使っていて、その後乙が引き継ぐなどのケースを想定しています）。よって原案のままとさせて頂きます。		
10	全般	令和9年度以降にシステムを利用することが考えられるシステムを調達する場合、二要素認証を必須要件とするという件について、システム全体を更新する場合はよいのですが、部分的な一部システムの更新の場合、例えば病院全体の医療情報システムではなく、透析室のシステムだけを更新する場合でも、二要素認証を採用することは、費用負担的に厳しいのではないでしょうか。機材の金額のみならず、多要素認証のシステム金額の負担・・・特に静脈認証等はハードウェアとシステムを含めて数千万レベルと高額なことがあり、全体的なシステムの更新ならば費用面の問題を吸収できても、単体の部分的なシステムでも必須となると、費用面で吸収できるものではなくなる可能性が高いと考えられます。医療機関等の全体的なシステム更新の場合のみの要件とすることはできないでしょうか。	今回の改定では、二要素認証導入の促進を図る観点から、今後新規導入、あるいは更新する医療情報システムに対して、原則として二要素認証の導入を図ることを目的とするものです。従って、医療情報システムの部分的な更新等であっても、原則として二要素認証対応を図ることが求められます。 なお本ガイドラインでは、医療情報システムが設置されている部屋において入退室管理を適切に行われている等、全体として二要素認証に相当する対応を講じることも、対応方法として認めております。この点からの検討も進めていただくことも想定されます。		
11	6.12	令和2年度診療報酬改定にて、事務の効率化・合理化を目的として「署名又は記名・押印を要する文書については、自筆の署名（電子的な署名を含む。）がある場合には印は不要である。」（令和 2 年 3 月 5 日保医発第 1 号の別添 1 項番 8）とされており、令和2年度診療報酬改定の概要（令和 2 年 3 月 5 日厚生労働省保険局医療課）においても医療機関における業務の効率化・合理化として、「文書による患者の同意を要件としているものについて、電磁的記録によるものでもよいことを明確化する。」となっている。これらから、例えば各種同意書への患者や医療従事者のサインは、タブレットやスマートフォン上で行う手書きのサイン等による電磁的な記録でよいものと判断しております。(改変が行われていないための真正性に担保する措置は必要)本章では、e-文書法の対象文書についての記載だが、前述について補記することで、より利用者に分かりやすい内容となると考えます。また、医療従事者や患者の効率化や負荷軽減のために、法令で署名又は記名・押印が義務付けられた文書等についても、タブレットやスマートフォン上で行う手書きのサイン等の電磁的記録を含めた形が可能な文書はないのか、是非本ガイドラインでの検討をお願いします。	本ガイドラインでは、法令で署名又は記名・押印が義務付けられた文書等については、6.12 章において定める電子署名によることとしています。これ以外のタブレットやスマートフォン上で行う手書きのサイン等の電磁的記録を含めた形が可能とする、法令で署名又は記名・押印が義務付けられた文書等はありません。また、本ガイドラインにおいて法令で署名又は記名・押印が義務付けられた文書等に関する扱いを記載することは混乱を生じさせるおそれがあるため、原案のままとさせて頂きます。		
12	8.1.2	e 項に一般財団法人医療情報システム開発センターの資格試験に合格し、一般社団法人医療情報安全管理監査人協会が認証した「公認医療情報システム監査人」も追記していただきたい。	8.1.2 c2.(9)e では、例示的な内容を示す目的であり、全ての資格等を列挙する趣旨ではありません。具体的な内容を QA に記載し、その中に反映しました。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
13	6.11	■意見の概要 『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。』の記述を、 『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、原則として使用せず、やむを得ず SSL-VPN を利用する場合は、TLS 暗号設定ガイドラインに基づき、「クライアント型」での SSL-VPN とすること』 に変更したほうが好ましい。 ■意見の理由 関連ガイドラインである、 『TLS 暗号設定ガイドライン 3.0.1 版』 『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』 ではいずれも、SSL-VPN を利用する場合は、クライアント型を採用することとされています。当該ガイドラインでも、クライアント型 SSL-VPN に関する上記記述を行うことで、ガイドライン間の記述ずれがなくなり、医療機関・事業者それぞれのガイドライン理解が深まり、その結果医療情報システムの普及に資するものと考えられます。 TLS 暗号設定ガイドライン 3.0.1 版 9.1 リモートアクセス VPN over SSL （いわゆる SSL-VPN）（83 ページ） 『クライアント型は（中略）、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ため、端末に IPsec-VPN ソフトをインストールして構成するモバイル型の IPsec-VPN に近い形での運用形態となる。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。』 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 脚注 22（28 ページ） 『また、SSL-VPN を原則として利用せず、やむを得ず SSL-VPN を利用する場合は、SSL/TLS 暗号設定ガイドラインに基づき、「クライアント型」での SSL-VPN とすること』 技術的観点からも、クライアント型 SSL-VPN であれば、偽サーバへの対策が十分可能と考えられます。	本ガイドラインで想定している医療機関等においては、必ずしも「偽サーバーへの接続可能性がないこと」などを確認できる知見ををを有しているとは限らないため、適切な判断が難しいことも想定されます。そこで、SSL-VPN については、原則として使用しないこととしています。なお、ご指摘を踏まえて、やむを得ず「クライアント型」での SSL-VPN を用いることで、偽サーバへ接続リスクが低い場合については、QA において示させていただきました。		
14	全体	e-gov のパブコメの文字数が 2000 文字に制限されているため、4 分割でコメントを入力します。 誤植等が残っているとその文書に作成、レビューの不足等を感じてしまい、せっかくすばらしいドキュメントが軽視されるおそれが発生してしまうのではと思います。 このため、非常に細かい点ですが、気付いた点を記します。 1.PDF をしおりつきで提供してほしい しおりを使うことにより、全体の構成でどこを読んでいるかがわかりやすい、また、別な章にも簡単に遷移できる。 また、作成も Word で(適切に見出しを設定して)作成してあれば、タグを含んで PDF 保存すればいいだけで手間もかからないはず。 さらに、しおりが設定されていない長文の PDF を公開することは、その PDF 作成者の IT リテラシに関して疑問を呈するものもいるかもしれない。(場合によっては、そのような状態のガイドラインを軽視されるおそれもあるかもしれない。) しおりを使った PDF の例 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(令和 2 年 8 月、総務省、経済産業省)	ご指摘を踏まえて、しおり機能を利用した形で公表させていただきます。		公開時にしおり機能対応
15	付表と QA	2.3 つの付表、Q&A 等も更新したものを公表してほしい。	ご指摘を踏まえて対応させていただきます。		付表等を公開

整理番号	章	意見	考え方	修正内容	
				原案	修正案
16	目次 6	3.目次 6 ＊6 章のタイトルを本文(P39)で修正しているので、目次の対応する部分も修正するか又は目次を全て更新が必要。 (変更前) 6. 情報システムの基本的な安全管理 (変更案) 6. 医療情報システムの基本的な安全管理	ご指摘を踏まえて対応させていただきます。	6. 情報システムの基本的な安全管理	6. 医療情報システムの基本的な安全管理 ※全体的に修正 例外 P15、P40。P46、P53(文書名、引用など)
17	目次 8.1.2	4.目次 8.1.2 ＊8.1.2 章のタイトルを本文(P118)で修正しているので、目次の対応する部分も修正するか又は目次を全て更新が必要。 (変更前) 8.1.2. 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 (変更案) 8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準	ご指摘を踏まえて対応させていただきます。	8.1.2. 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準
18	改定履歴	5.P4 改定履歴 改定履歴の表で、一番左の列(版数)の列幅をもう少し広くしたほうがいい。第 4.1 版、第 4.2 版等で、”版”の前で改行がはいってしまって醜い。安全管理ガイドライン第 5 版では、適切になっていた。	改行が入らないよう、調整させていただきます。		※表内設定調整
19	改定履歴	6.P7 改定履歴 5.1“また、近時のサイバー攻撃などへの対応に求められる措置として、ネットワークの監視等の管理に関する措置やネットワークの構築のあり方、外部からのデータ取り込みにおける対応措置等の必要性について”と記載されているが、7.1 では、”取り込み“を“取込み”と修正している。これと合わせた修正が必要ではないか。7.1 の B-1 の記載も同様。	ご指摘を踏まえて対応させていただきます。	改定履歴 5.1 また、近時のサイバー攻撃などへの対応に求められる措置として、ネットワークの監視等の管理に関する措置やネットワークの構築のあり方、外部からのデータ取り込みにおける対応措置等の必要性について 7.1 B-1※ 記録の確定とは、入力者により入力された情報に対して、確定を実施する権限を有する確定者によって入力の完了が確認されることや、検査、測定機器による出力結果の取り込み完了することをいう。	改定履歴 5.1 また、近時のサイバー攻撃などへの対応に求められる措置として、ネットワークの監視等の管理に関する措置やネットワークの構築のあり方、外部からのデータ取込みにおける対応措置等の必要性について 7.1 B-1※ 記録の確定とは、入力者により入力された情報に対して、確定を実施する権限を有する確定者によって入力の完了が確認されることや、検査、測定機器による出力結果の取込みが完了することをいう。
20	2	7. P14 2 章 “巻末の 3 つの付表“と記載あるが、巻末には表がない。第 5 版から別紙になっている。 別添の 3 つの付表とかにしたほうがいいのでは。その 3 つの付表も修正し、公開が必要ではないか。	ご指摘を踏まえて、本ガイドライン公表時に、別紙として、併せて公表させていただきます。	付表 1 一般管理における運用管理の実施項目例 付表 2 電子保存における運用管理の実施項目例 付表 3 外部保存における運用管理の例	別紙 付表 1 一般管理における運用管理の実施項目例 付表 2 電子保存における運用管理の実施項目例 付表 3 外部保存における運用管理の例 ※公開対応予定
21	3.4	8. 3.4 誤植 “9.5 (捕捉) 運用の利便性~“と記載あるが、”補足“の誤植である。	ご指摘を踏まえて対応させていただきます。	9.5 (捕捉) 運用の利便性	9.5 (補足) 運用の利便性
22	6.11	9. 6.11.C.6 “通信事業者”は、本書内では一貫して“電気通信事業者”にしたほうがいい。 6.11.C.8 も同様	ご指摘を踏まえて対応させていただきます。	通信事業者	電気通信事業者 P.94,95 を修正
23	4.2.1	10. P25 4.2.1 (1)事後責任について →(1)となっているが(2)の間違い	ご指摘を踏まえて対応させていただきます。	4.2.1 (1)事後責任について	4.2.1 (2)事後責任について
24	4.3	11. P30 4.3(4) 言葉が変 “障害等の非常時が発生した場合に”→障害等が発生した非常時の場合に	ご指摘を踏まえて対応させていただきます。	障害等の非常時が発生した場合に	障害等の発生した非常時の場合に

整理番号	章	意見	考え方	修正内容	
				原案	修正案
25	4.3	12.　P31 4.3(4)　言葉が変 (変更前) 　1 者および複数の事業者と受託する場合の責任分界の考え方 (変更案) 　1 者または複数の事業者が受託する場合の責任分界の考え方	ご指摘を踏まえて対応させていただきます。	1 者および複数の事業者と受託する場合の責任分界の考え方	1 者または複数の事業者と受託する場合の責任分界の考え方
26	4.4	13.　P33 4.4 組織が任意団体から一社になり、英語の表記が少し変わった。 (変更前) 医療情報標準化推進協議会(Health Information and Communication Standrds Board : HELICS 協議会) (変更案) 一般社団法人　医療情報標準化推進協議会(Health Information and Communication Standrds Organization : HELICS 協議会)	ご指摘を踏まえて対応させていただきます。	医療情報標準化推進協議会(Health Information and Communication Standrds Board : HELICS 協議会)	一般社団法人医療情報標準化推進協議会(Health Information and Communication Standrds Organization : HELICS 協議会)
27	6.1	14.　P40 6.1 “個人情報の取　扱い”と記載され、“取”と”扱い“との間に空白？がはいってしまっている。	ご指摘を踏まえて対応させていただきます。	個人情報の取　扱い	個人情報の取扱い
28	6.1	15.　P40 6.1 A.3.2.2　“明記しなければならない。”の明記の後に改行がはいってしまっている。	ご指摘を踏まえて対応させていただきます。		改行削除
29	6.2.3	e-gov のパブコメの文字数が 2000 文字に制限されているため、4 分割でコメントを入力します。 16.　P46 6.2.3 まる 7 (b) “プログラム上の欠陥”とあるが、“ソフトウェア上の欠陥”にしたほうがいいのでは。 “プログラム”はその本来の意味で、“手順の計画“のような意味もある。ここでは、(バグ)とあるので、コンピュータプログラムであり、他の部分に合わせて”ソフトウェア“に統一したほうがいいと思われます。 本書では、“プログラム”の言葉を本来の”手順の計画“の意味で使っている部分もある。 下記の 8.4.2, 付則 1, 付則 2 の 3 か所。これらは、このまま。	ご指摘を踏まえて対応させていただきます。	プログラム	ソフトウェア P.46,64,128,152,160 を修正
30	6.2.3	17.　P46 6.2.3 まる 7 (b) “・故障”の後に“外部サービスの利用~”がつながってしまっている。“故障”の後に改行を追加して、“・外部サービスの利用～”のように新規箇条にすべき。 参考として、第 5 版での該当箇所の記載。5.1 では情報漏えいを(b)の IT 障害以外として、変わりに“～ポリシー等の変更等”を追加したものと思われる。	ご指摘を踏まえて対応させていただきます。	・ 故障 ・ 外部サービスの利用に伴うシステムポリシー等の意図しない変更等	・ 故障 ・ 外部サービスの利用に伴うシステムポリシー等の意図しない変更等
31	6.5	18.　P51 6.5 (1) (1)のタイトルの“利用者の識別及び認証”を”利用者の識別・認証”に修正しているが、B の後には、(1)利用者の識別及び認証になったままで、あっていない。これらは、まったく同じものなので、同じ記載にすべき。また、本ガイドラインの全体を通して、一貫して同じ使いかたになるようにすべき。	ご指摘を踏まえて対応させていただきます。	利用者の識別及び認証	利用者の識別・認証 P.51,104,105 を修正
32	6.5	19.　P53 6.5 B 二段階の“二”が赤文字になってしまっている。(複数個所あり)　通常の黒文字でいいのではないか。	ご指摘を踏まえて対応させていただきます。		黒字に変更
33	6.5	20.　P53 6.5 B “「類推しやすいパスワードを使用しない」”は、関係する C 項(C.12.(5))の表現を修正しているので、それに合わせた修正。 (修正案) “「類推されやすいパスワードを使用しない」”	ご指摘を踏まえて対応させていただきます。	類推しやすい	類推されやすい
34	2.1	21.　遵守 vs 順守　今回の修正で、順守を遵守に修正されている箇所が散見される、本ガイドライン内で統一して、”遵守”を使用したほうがいいのでは。順守を使っている箇所(1) P11 4 箇所(2) P149 付則 1.2　C.1(3)	ご指摘を踏まえて対応させていただきます。	順守	遵守 P.11,149 を修正
35	6.5	22.　P62 6.5.D.6　誤植 “組み合わるなど”→“組み合わせるなど”	ご指摘を踏まえて対応させていただきます。	組み合わるなど	組み合わせるなど

整理番号	章	意見	考え方	修正内容	
				原案	修正案
36	6.6	23. P64 6.6.C.2.(1) a のみ、文章の最後の“こと”の後に句点(“。”)がない。他に合わせて句点(“。“)を追加。	ご指摘を踏まえて対応させていただきます。	a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること	a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。
37	6.6	24. P64 6.6.C.2.(2) “プログラムの異常等で”→“ソフトウェアの異常等で”にしたほうがいいのでは。	ご指摘を踏まえて対応させていただきます。	プログラムの異常等	ソフトウェアの異常等
38	6.9	25. P70 6.9.C.8 “持ち出した情報機器をネットワークに接続したり、他の外部媒体をネットワークに接続する場合“は、言葉がわかりにくい。例えば、“持ち出した情報機器をネットワークに接続したり”は、持ち出したものを持ち出した先で、外部のネットワークに接続することを想定しているのか、あるいは、持ち出したものを持ち帰って、医療施設等のネットワークに接続することを想定しているのかわかりにくい。同様に読点の後半も同様。 外部持ち出しで考慮しなければいけない場合は、下記 5 パターン (1) 持ち出した情報機器を外部のネットワークに接続 (2) 持ち出した情報機器に外部の外部媒体を接続 (3) 持ち出した外部媒体を外部の情報機器に接続 (4) 持ち出した情報機器を持ち帰り、施設内のネットワークに接続 (5) 持ち出した外部媒体を持ち帰り、施設内のネットワークに接続されている情報機器に接続 ここの C.8 ではウイルス対策ソフト、パーソナルファイアウォールを対策例としているので、上記の(1)、(2)。これを誤解しないように記載する必要がある。 （変更案） 持ち出した情報機器を外部のネットワークに接続したり、他の外部媒体を接続したりする場合は、	ご指摘を踏まえて、一部表現の見直しをさせていただきます。	8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体をネットワークに接続する場合は、	8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体をネットワークに接続したりする場合は、
39	6.9	26. P70 6.9.C.8 誤植 “公衆無線 LAN は 6.5 章 C.13 の基準を満たさない“と記載されているが、C.14 へ修正が必要。	ご指摘を踏まえて対応させていただきます。	公衆無線 LAN は 6.5 章 C.13 の基準を満たさない	公衆無線 LAN は 6.5 章 C.14 の基準を満たさない
40	6.11	27. P89 6.11 B-2 Ⅲ 1) “携帯電話・PHS 網に接続ケースである。” -> “携帯電話・PHS 網に接続するケースである。”	ご指摘を踏まえて対応させていただきます。	携帯電話・PHS 網に接続ケースである。	携帯電話・PHS 網に接続するケースである。
41	6.11	28. P90 6.11 B-2 Ⅲ 2) “インターネット経由で医療機関等のアクセスポイント接続するケースである。”と記載されているが、下記の(変更案)にように、助詞(“に”)を補ったほうが自然な文ではないか。 (変更案) “インターネット経由で医療機関等のアクセスポイントに接続するケースである。”	ご指摘を踏まえて対応させていただきます。	インターネット経由で医療機関等のアクセスポイント接続するケースである。	インターネット経由で医療機関等のアクセスポイントに接続するケースである。
42	6.11	29. P93 6.11 B-3 句点(“。”)が抜けてしまっている。	ご指摘を踏まえて対応させていただきます。	送信先／アップロード先についての安全性等を確認し、疑義が生じた場合に患者からの依頼を断るなどのほか、送信等を行うに当たっては、患者との関係で責任分界についても取り決めておくことが求められる	送信先／アップロード先についての安全性等を確認し、疑義が生じた場合に患者からの依頼を断るなどのほか、送信等を行うに当たっては、患者との関係で責任分界についても取り決めておくことが求められる。
43	6.12	e-gov のパブコメの文字数が 2000 文字に制限されているため、4 分割でコメントを入力します。 30. P98 6.12. C.1 (2) “A の要件を満たす“→”A 項の要件を満たす“	ご指摘を踏まえて対応させていただきます。	A の要件を満たす	A 項の要件を満たす
44	7.1	31. P104 7.1 B-2 (1) 6.5 章の利用者の識別及び認証は、6.5 章の記載が変わったので、それに合わせて、”利用者の識別・認証”にすべき。 同様の箇所が前 Page(P103)にもあり。	ご指摘を踏まえて対応させていただきます。	6.5 章の利用者の識別及び認証	6.5 章の利用者の識別・認証
45	7.1	32. P105 7.1 C.1 他の修正に合わせて、“識別及び認証”を“識別・認証”に修正したほうがいいのではないか。	ご指摘を踏まえて対応させていただきます。	識別及び認証	識別・認証

整理番号	章	意見	考え方	修正内容	
				原案	修正案
46	7.1	33. P107 7.1. C.7 以下の文を修正したほうが日本語が自然になるのでは。 平文化ではなく、暗号化と対にして復号、“や”はあいまいなため、できるだけ避ける。Or の併記で最後に“等”があるので、併記ではなくリスト表現にする。 (変更前) “圧縮・解凍又はセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにあたらない。“ (変更案) “圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにあたらない。“	ご指摘を踏まえて対応させていただきます。	圧縮・解凍又はセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにあたらない。	圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにあたらない。
47	7.2	34. P110 7.2. B 以下の文を修正したほうが日本語が自然になるのでは。 (変更案) そのため、電子媒体に保存された情報は、保存された～	ご指摘を踏まえて対応させていただきます。	電子媒体に保存されたこれらに適切に対応することにより、	電子媒体に保存された情報は、保存されたこれらに適切に対応することにより、
48	7.3	35. P115 7.3. D.1.(1) 誤植 “保管ずるとともに”→“保管するとともに”	ご指摘を踏まえて対応させていただきます。	保管ずるとともに	保管するとともに
49	8.1.2	36. P118 8.1.2 A 誤植 (安全管理措置)の後の 2 行のフォントが他と異なる。あるいは、Bold になってしまっている。	ご指摘を踏まえて対応させていただきます。		書式を変更
50	8.1.2	37. P119 8.1.2 B.1.まる 2 誤植 “~ことなどの有効である”→“~ことなどが有効である。”	ご指摘を踏まえて対応させていただきます。	ことなどの有効である	ことなどが有効である
51	8.1.2	38. P120 8.1.2 B.2.まる 1 8.1.2.C.1.(3)の修正と同じ修正が必要では。 ”不当な営利、利益“→”不当な利益“	ご指摘を踏まえて対応させていただきます。	不当な営利、利益	不当な利益
52	8.1.2	39. P120 8.1.2 B.2.まる 2 8.1.2.C.1.(3)の修正と同じ修正が必要では。 ”不当な営利、利益“→”不当な利益“	ご指摘を踏まえて対応させていただきます。	不当な営利、利益	不当な利益
53	8.1.2	40. P120 8.1.2 B.2.まる 2 “実施されないことの確認、若しくは実施させないことを“となっているが、JIS や法文等の記載方法に合わせて、or が 1 階層の場合は、”又は“を使うのが望ましいのでは。 “若しくは”→又は	ご指摘を踏まえて対応させていただきます。	実施されないことの確認、若しくは実施させないことを	実施されないことの確認、又は実施させないことを
54	8.1.2	41. P121 8.1.2 B.3.まる 2 “医療機関等若しくは医療機関等との間で同意を得た患者” “若しくは”→又は	ご指摘を踏まえて対応させていただきます。	医療機関等若しくは医療機関等との間で同意を得た患者	医療機関等又は医療機関等との間で同意を得た患者
55	8.1.2	42. P122 8.1.2 C.1.(5) 誤植 “配慮よう求める”→“配慮するよう求める”	ご指摘を踏まえて対応させていただきます。	配慮よう求める	配慮するよう求める
56	8.1.2	43. 8.1.2 C.2.(9).e 下記を JASA クラウドの上に追加 “ISO/IEC 27017 による認証取得” (参考)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から抜粋	8.1.2 c2.(9)e では、例示的な内容を示す目的であり、全ての認証、資格等を列挙する趣旨ではありません。具体的な内容を QA に記載し、その中に反映しました。		
57	8.1.2	44. P123 8.1.2 C.2.(9).e 誤植 ・AICPA SOC3(SysTrust/WebTrsuts)(日本公認会計士協会 IT2 号) 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でも同じ誤植のようですが。 正しくは、WebTrust 出典として記載されている「日本公認会計士協会 IT2 号」では、“WebTrust” (参考)「日本公認会計士協会 IT2 号」 抜粋 https://jicpa.or.jp/specialized_field/files/2-10-2-2-20140116.pdf	ご指摘を踏まえて対応させていただきます。	・AICPA SOC3(SysTrust/WebTrsuts)(日本公認会計士協会 IT2 号)	・AICPA SOC3(SysTrust/WebTrust)(日本公認会計士協会 IT2 号)
58	8.1.2	45. P123 8.1.2 D.2. 誤植 “医療機関等の以外外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合“→” 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合“	ご指摘を踏まえて対応させていただきます。	医療機関等の以外外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合

整理番号	章	意見	考え方	修正内容	
				原案	修正案
59	9.1	46.　P130 9.1 B （2） 　~一貫した運用ができない場合、及びオーダエントリーシステムや”と、記載あるが、“及び“より、”又は“にしたほうが自然な表現になるのではないか。 　“及び”→”又は”に修正	ご指摘を踏まえて対応させていただきます。	一貫した運用ができない場合、及びオーダエントリーシステムや	一貫した運用ができない場合、又はオーダエントリーシステムや
60	9.2	47.　P133 9.2 C.1 (1) 誤植 　”~時点で遅滞なく必要がある。“→　”~時点で遅滞なく行う必要がある。“	ご指摘を踏まえて対応させていただきます。	時点で遅滞なく必要がある。	時点で遅滞なく行う必要がある。
61	10	48.　P139 10 C 1.(4) f 　“リスクに対する予防、発生時の対応方法” 　　6.3 C.5 の記載と合わせたほうがいいのでは。 　“リスクに対する予防措置、発生時の対応方法”	ご指摘を踏まえて対応させていただきます。	リスクに対する予防、発生時の対応方法	リスクに対する予防措置、発生時の対応方法
62	付則	e-gov のパブコメの文字数が 2000 文字に制限されているため、4 分割でコメントを入力します。 49.　P146　付則 1 “これに加え、搬送時や外部保存を受託する事業者における取扱いに特に注意する必要がある。”と記載あるが、“特に”と記載あるので、“事業者における取扱い”一般ではなく、その後に記載のある、“障害等”を明記したほうがいいのでは。今回の改定前では、“事故発生時”と表現していた。 (変更案) “これに加え、搬送時や外部保存を受託する事業者の障害等に対する取扱いに特に注意する必要がある。” 以上です。	ご指摘の部分ですが、一般的に「搬送時や外部保存を受託する事業者における取扱いに注意する必要」すべきこと示す目的ですので、ご指摘箇所のうち「特に」を削除して対応させていただきます。	診療録等を医療機関等の内部に電子的に保存する場合に必要とされる真正性、見読性、保存性を確保することで概ね対応が可能と考えられるが、これに加え、搬送時や外部保存を受託する事業者における取扱いに特に注意する必要がある。	診療録等を医療機関等の内部に電子的に保存する場合に必要とされる真正性、見読性、保存性を確保することで概ね対応が可能と考えられるが、これに加え、搬送時や外部保存を受託する事業者における取扱いに注意する必要がある。
63	6.5	6.5(1) 利用者の識別・認証について ID/パスワードに加えた二要素目の認証方式として、ワンタイムパスワードの利用も一つの選択肢として有効と考えます。スマーフォンのアプリを利用したワンタイムパスワード方式であれば、スマートフォンへのログインに生体認証(指紋認証または顔認証)が行われることで利用者が特定できます。さらにワンタイムパスワードアプリによる認証が加わることで、より強固な認証になりえると考えます。	ご指摘の箇所は例示として示すものであり、、ワンタイムパスワードを排除する趣旨ではございません。原案のままとさせていただきます。		
64	6.5	6.5(4) 不正アクセス対策について最近のサイバー攻撃は巧妙化しており、検出するためのパターンファイルや検索エンジンを最新のものに更新して脆弱性へのパッチ適用を行っても、未知の攻撃に対して有効な対策を実施することは困難です。端末内の振る舞い検査機能や端末内のアクティビティを記録する EDR の導入を推奨すべきであると考えます。また、ゼロディ攻撃で利用される実行型ファイルのランサムウェアなどは、振る舞い検査等で検出が難しいケースもあり、サンドボックスによるマルウェア判定が必要になるケースもあります。従いまして、サンドボックス検査に基づいたクライアント端末での感染防御の仕組みも有効性が高いと考えます。	ご指摘の内容につきましては、6.5　B(5)などで考え方を示させて頂いております。具体的なソリューションについては記載する趣旨ではありませんので、原案のままとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
65	6.5	6.5(5)ネットワーク上での不正アクセスについて 暗号化したデータ通信はセキュリティ対策の一環として重要な対策方法ですが、一方で データが暗号化されていることにより IDS/IPS によるコンテンツスキャンやマルウェアチェックを十分に行うことができず、脅威検知を十分にできなくなってしまいます。最近ではインターネット通信の 80%が SSL 通信になっており、SSL 復号による可視化の検討が必要だと考えます。 6.5(6)医療等分野における IoT 機器の利用について 医療用機器やウェアラブル端末などの IoT デバイスは、デバイス上にソフトをインストールすることが困難であり、不正アクセス対策を十分に行うことができません。一方で IoT デバイスはサポート切れの古い OS が稼働しているケースが多く、十分なセキュリティ対策が行えていないケースが多いため、ネットワーク上での IoT デバイスを識別する仕組みに加えて IoT デバイスに対する攻撃を検知するための対策を講じることが重要であること考えます。 また、D.推奨されるガイドラインの(3)の箇所になりますが、IP アドレスやポート番号だけでは十分なアクセス制御が難しく、また調査段階におけるログ情報としても不十分なケースが多く、調査の負荷増大と対応時間の長期化につながります。そのため、アプリケーションによる識別やユーザ識別などに基づく ACL を推奨いたします。 6.10(3) サイバー攻撃を受けた際の非常時の対応について 非常時の対応のみではなく、医療業務の復旧後、再発防止策として、感染ルートや感染源、さらに影響範囲の特定なども重要であると考えます。また、それらを行うための仕組みも必要であると考えます。サイバー攻撃を受けた場合、まずは現場では復旧優先で対処が行われる為、サイバー攻撃を把握して調査するための情報が十分に収集できないことが想定されます。それらの懸念に対しての対策としては、平常時から常時端末のアクティビティ情報やネットワークのトラフィック情報を記録しておき、分析調査ができる EDR のような仕組みが必要であり、ゼロトラストという概念においても重要視されています。 6.11.B-2 選択すべきネットワークのセキュリティの考え方について 閉域網からのアクセスにおいても、感染端末からのアクセスや不正アクセスなどのリスクが存在するため、なりすましを防ぐセキュリティ対策の実施に加えて、すべての記録を行うことが重要だと考えます。また、テレワークに関しては、端末と医療情報システム間のセキュリティ対策だけでなく、テレワーク端末からのインターネット通信を含むすべての通信に対するアクセス制御の実施と記録が重要だと考えます。また、「オープンなネットワークで接続する場合」の箇所に記述されている無害化ですが、1つの対策方法に過ぎないため、未知の脅威対策や、無害化の実施、早期検知と早期対応の仕組みを導入するといった記述の方がより実環境にあった対策が検討できるものと考えます。 6.11.C 最低ガイドラインについて 11 の箇所になりますが、未知の攻撃に対する対策や、100%攻撃を防ぐことができないことを前提にした検知の仕組み対策を講じることが重要であると考えます。	参考意見として承りました。		
66	6.5	6.5(6)医療等分野における IoT 機器の利用について 医療用機器やウェアラブル端末などの IoT デバイスは、デバイス上にソフトをインストールすることが困難であり、不正アクセス対策を十分に行うことができません。一方で IoT デバイスはサポート切れの古い OS が稼働しているケースが多く、十分なセキュリティ対策が行えていないケースが多いため、ネットワーク上での IoT デバイスを識別する仕組みに加えて IoT デバイスに対する攻撃を検知するための対策を講じることが重要であること考えます。 また、D.推奨されるガイドラインの(3)の箇所になりますが、IP アドレスやポート番号だけでは十分なアクセス制御が難しく、また調査段階におけるログ情報としても不十分なケースが多く、調査の負荷増大	医療用機器については、ネットワーク対策と併せてリスク対応しているおります。参考意見として承りました。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		と対応時間の長期化につながります。そのため、アプリケーションによる識別やユーザ識別などに基づくACLを推奨いたします。			
67	6.10	6.10(3) サイバー攻撃を受けた際の非常時の対応について 非常時の対応のみではなく、医療業務の復旧後、再発防止策として、感染ルートや感染源、さらに影響範囲の特定なども重要であると考えます。また、それらを行うための仕組みも必要であると考えます。サイバー攻撃を受けた場合、まずは現場では復旧優先で対処が行われる為、サイバー攻撃を把握して調査するための情報が十分に収集できないことが想定されます。それらの懸念に対しての対策としては、平常時から常時端末のアクティビティ情報やネットワークのトラフィック情報を記録しておき、分析調査ができるEDRのような仕組みが必要であり、ゼロトラストという概念においても重要視されています。	ご指摘の部分では、復旧後の対応も含めて、BCP対策をする必要性を示しております。参考意見として承りました。		
68	6.11	6.11.B-2 選択すべきネットワークのセキュリティの考え方について 閉域網からのアクセスにおいても、感染端末からのアクセスや不正アクセスなどのリスクが存在するため、なりすましを防ぐセキュリティ対策の実施に加えて、すべての記録を行うことが重要だと考えます。また、テレワークに関しては、端末と医療情報システム間のセキュリティ対策だけでなく、テレワーク端末からのインターネット通信を含むすべての通信に対するアクセス制御の実施と記録が重要だと考えます。また、「オープンなネットワークで接続する場合」の箇所に記述されている無害化ですが、1つの対策方法に過ぎないため、未知の脅威対策や、無害化の実施、早期検知と早期対応の仕組みを導入するといった記述の方がより実環境にあった対策が検討できるものと考えます。	テレワークの実施においても、医療情報を取り扱う場合には、本ガイドラインを遵守する必要があり、指摘いただいた内容も含めて適切な対応をとることを想定しております。		
69	6.11	6.11.C 最低ガイドラインについて 11の箇所になりますが、未知の攻撃に対する対策や、100%攻撃を防ぐことができないことを前提にした検知の仕組み対策を講じることが重要であると考えます。	ご指摘の趣旨は、本ガイドラインの6.5B(5)により、考え方を示させて頂いております。		
70	6.5	・p52＜認証強度の考え方＞中、「医療情報システムにアクセスする端末ごとに二要素認証を追加実装」「医療情報システムを利用する端末に二要素認証が実装」といった表現になっているが、「端末」にとすると範囲が不適切に限定される可能性がある（二要素認証を機能として提供するのは「システム」と考える）ため、端末とせず、例えば、「医療情報システムを利用する端末に」であれば「医療情報システムに」とすべきではないか。	ご指摘を踏まえて対応させていただきます。	医療情報システムを利用する端末に二要素認証が実装されていないとしても、	医療情報システムに二要素認証が実装されていないとしても、
71	6.5	・p55 「(2) 情報の区分管理とアクセス権限の管理」中、「意図せぬ設定の変更に関して検知できる措置を講じることが求められる。特に自動的に検知し、運用に反映できることが必要となる。」とあるが、意図せぬ設定の変更というのを事前定義することは非常に難しいと考えるため、「権限や設定の変更の際には、変更による影響を確認する手順を設け、意図しない変更を無くす運用が必要となる。」としてはどうか。	ご指摘の箇所につきましては、クラウドサービスを利用する場合、利用するサービスによっては、医療機関等の規程に基づいて定めたシステム上の設定（ポリシー）が、デフォルトの設定となる等、自動的に意図しない内容に変更されてしまうケースを踏まえて記述しております。ここにいう「意図せぬ」は、「想定外」の意味ではなく「システム管理者が予定していない（発生が検知されれば対応できる）自動変更」の意義として用いており、事前定義が必ずしも難しい場面ではないケースを想定しております。そこで、原案の通りとさせていただきます。		
72	全般	令和2年度診療報酬改定の概要(3/5改訂版)のP25に、文書による患者の同意を要件としているものについて、電磁的記録によるものでもよいことを明確化する。という記述があります。 今回のガイドライン第5.1版でも同様の記述をされ、例えば同意書など紙で行われていた署名に対し、ペンタブレットなど使った電子サイン(正副の副ではなく、最初から電磁的記録として電子的に医師や患者がサインする)を認めることはないのでしょうか。 昨今のハンコレス、デジタル化の流れに沿うものであり、医療機関からも電子サイン化を望む声が数多くあることから、意見として提出を致します。よろしくお願い致します。	本ガイドラインでは、法令で署名又は記名・押印が義務付けられた文書等については、6.12章において定める電子署名によることとしています。これ以外のタブレットやスマートフォン上で行う手書きのサイン等の電磁的記録を含めた形が可能とする、法令で署名又は記名・押印が義務付けられた文書等はありません。また、本ガイドラインにおいて法令で署名又は記名・押印が義務付けられた文書等に関する扱いを記載することは混乱を生じさせるおそれがあるため、原案のままとさせて頂きます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
73	6.11	P86 に記載されている「無害化について」 総務省のガイドラインのような、無害化に関する必須技術要件を明確にしてください。 例）無害化後の再編集（再利用）、フォーマットに基づいた構成要素での再構成 （単純にマクロコードの削除ではない）など。	本ガイドラインで想定している「無害化」について、用語集にて定義しました。		
74	2	<項番 1><14 頁 2 章> <該当箇所> なお、巻末の 3 つの付表は、 <意見内容> 巻末の 3 つの付表及び付録がパブコメとして公開されていませんが、第5版と同様としてよいでしょうか。 <理由>目次には記述されているが、パブコメとして公開されていない為	巻末の 3 つの付表は、公開することを予定しております。		
75	4.3	<項番 2>< 28 頁 4.3.(1)(b)2> <該当箇所> ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン(a)1に沿った考え方の整理が必要である。 <意見内容> 該当ガイドラインで(a)1 が見つからない。参照先が異なっているのではないでしょうか? 該当ガイドラインでは責任分界点に対する整理を述べている箇所が無いように見受けられます。 「*****ガイドラインを参考に(a)1 に沿った考え方の整理が必要である。」というようなことでしょうか。。 <理由> JAHIS 基本データセット適用ガイドラインでは該当箇所がにつからず、参照箇所の記述違いと思われるため	ご指摘の箇所は、誤植ですので、「一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン」を削除します。	ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン(a)1に沿った考え方の整理が必要である。	ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、(a)1に沿った考え方の整理が必要である。
76	8.1.2	<項番 3><119 頁 8.1.2.B.1.2> <該当箇所> 下から 3 行目 「外部保存されている医療情報は」の前に追記 <意見内容> 以下を追記する。「また、医療情報システム等の安全管理に係る評価に関しては、提供事業の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）による、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）の評価結果を確認することが望ましい。」 <理由> 「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」の「P20 4.3. 医療情報システム等の安全管理に係る評価」の記述と整合性を取るため。	ご指摘の箇所は、例示として参照文書を示させていただく趣旨であり、全ての参考文書を示す趣旨ではございませんので、原案の通りとさせていただきます。		
77	8.1.2	<項番 4><120-121 頁 8.1.2.B.2.2> <該当箇所> ”この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならない。”以降 <意見内容> 具体的方法である「暗号化を行う」に関する事項のみになっているため、その他の方法に対する記載を加えてはどうか? <理由>具体的方法として、「情報を分散保管する」方法も記述されている。ガイドラインの読みやすさのため	ご指摘の箇所は、例として挙げた対策のうち、さらに暗号化に関するものを具体的な内容例として召す趣旨であり、全ての具体例を示す趣旨ではありませんので、原案の通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
78	8.1.2	<項番 5><123 頁 C.2.(9)e><該当箇所>e 項全体<意見内容><< >>部の追加<<「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」の「第三者認証等の取得に係る要件」及び、>>「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。<<−プライバシーマーク認定−ISMS 認証パブリック・クラウドに関しては以下も推奨される。>>−JASA クラウドセキュリティ推進協議会 CS ゴールドマーク−米国 FedRAMP 以下原文通り。<理由>本要求事項の目的は「技術及び運用管理能力の有無の確認」であるが「下記に記述されたいづれかの認証を受けていることを要求している。一方、C.2.(3)では「提供事業者における安全管理ガイドライン」を遵守したシステムてはサービスの利用が必須となっていて、その P20 4.4. では、「プライバシーマーク認定または ISMS 認証を取得すること。」が必須となっている。2種類の認証を取ることを要求されことになり、提供事業者には負担になり、コスト高となり、また大手クラウドに有利になり、クラウドシステムの発展を推進することを阻害する。システム監査技術者や CISA による個人的でも良いとしているが、ISO27017 相当の監査をもとめる場合はそれなりの費用と時間がかかる。また、「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 4.2」ではプライベイトクラウドに関しては****が推奨される」となっていて政府調達では必須ではない。これらの要求事項と本ガイドラインの要求レベルを勘案する必要がある。<備考>なお、8.1.2.D.1. において、「個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークや ISMS 認定等の第三者による認定を取得している事業者を選定すること。」として、推奨事項として同様な記述があり、上記の C 項としての必須項目と重なってしまうが、この項は、「病院、診療所、医療法人等が適切に管理する場所に保存する場合」も含めた要求事故と解釈すれば、齟齬はないと考える。	本項は確認事項であり、必須事項ではありません。なおご指摘を踏まえて、JIS Q 27001、JIS Q 15001 について、8.1.2 c2.(9)e として確認内容として追記し、従来の 8.1.2 c2.(9)e は示し、従来の 8.1.2 c2.(9)f として項番を繰り下げました。	d 財務諸表等に基づく経営の健全性 e 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク・米国 FedRAMP・AICPA SOC2（日本公認会計士協会 IT7 号）・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。・システム監査技術者・Certified Information Systems Auditor ISACA 認定 f 医療情報を保存する機器が設置されている場所(地域、国)g 受託事業者に対する国外法の適用可能性	d 財務諸表等に基づく経営の健全性 e JIS 15001、JIS Q 27001 の認証の有無 f 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク・米国 FedRAMP・AICPA SOC2（日本公認会計士協会 IT7 号）・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。・システム監査技術者・Certified Information Systems Auditor ISACA 認定 g 医療情報を保存する機器が設置されている場所(地域、国)h 受託事業者に対する国外法の適用可能性
79	全般	医療現場の事務負担を極力抑え、医療業務に専念できるよう、セキュリティは厳重に高レベルに維持しながら、進めてください。	参考意見として承りました。		
80	6.2	・「6.2. 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」−C 項−No5 には、経産省・総務省 GL に基づき、医療機関等が IT 事業者より技術対策等の情報を収集することを求めている。一方、改定後の経産省・総務省 GL では IT 事業者は、自社システムの機能を用いて、医療機関へ実施を依頼すべき対策を伝えることを求めている。この主旨を鑑みると、医療機関等には「情報を収集」することでなく、「収集した情報に基づきリスク評価を行い、事業者と協議の上で、医療機関等が実施すべき対策を決定する」ことが要求されると思われる。そのためその観点で修正することが望ましい。（「収集する」ことを前面に出す表現の場合、「収集する」こと自体が目的化するおそれがあるため）	ご指摘に関して、6.2 項では、リスクアセスメントを行うことを想定した内容となっており、C.5 の記述もその観点で記載しているものであることはご認識の通りです。逆に情報収集は、ベンダーとのリスク調整などの観点からも行う可能性があるため、リスク分析目的に限定されないことも予想されます。よって原案通りとさせていただきます。	fa	
81	6.2	・上記の内容に関連するが、「6.2. 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」の B 項のなかに、改定後の経産省・総務省 GL を踏まえた観点から、なぜ技術情報を医療機関等が収集する必要があるのかについての記載が不足していると思われる。（JAHIS の MDS を紹介するのみ等、改定前の文章立て付けになっている） よって、改定後の経産省・総務省 GL の中で IT 事業者は技術情報やそれに基づく医療機関への依頼事項を提示することが求められている点、そのため医療機関等はそれに応えて、IT 事業者との間でリスクコミュニケーションを実施することが求められている点を明記することが必要と思われる。（事業者が経産省・総務省 GL に基づきリスクコミュニケーションを行おうとしても医療機関等にその必要性の認識がなく拒まれれば、コミュニケーションが成立しないリスクがあるため）	経産省・総務省 GL では、ベンダーに医療機関等とのリスクコミュニケーションを求めておりますが、ベンダーの情報開示に対して、一律に医療機関に回答義務を負担させるのは、、医療機関側に十分な情報システムに関する知見がある場合等の場合には、却って過度な負担となる恐れがあります。原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
82	8.1.2	「8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」-D 項-No1 では、医療機関等に「プライバシーマークや ISMS 認定等の第三者による認定を取得している事業者を選定すること」が推奨事項として求められている。一方、改定後の経産省・総務省 GL の「4.4. 第三者認証等の取得に係る要件」(p.20)では「医療情報を取り扱う事業者として、最低限の適格性を医療機関等へ示すため、(…)プライバシーマーク認定または ISMS 認証を取得すること」との記載がある。プライバシーマークや ISMS 認定は、事業者にとっては最低限の要求事項(C 項に該当)である一方、医療機関等が事業者を選定する際には必ずしも考慮する必要がないという点で、厚労省 GL と経産省・総務省 GL が相反する内容となっている。よって、8.1.2-D-No1 の項目は推奨事項ではなく、最低限の事項(C 項)に含めるべきと思われる。あるいは、C-(9)-e の「適切な外部保存に求められる技術及び運用管理能力の有無」を判断するための一例に位置付けるべきかと思われる。(P マークや ISMS 認定の位置付けが医療機関/事業者向けガイドラインで異なることで、混乱を招くリスクがあるため)	本項は確認事項であり、必須事項ではありません。なおご指摘を踏まえて、JIS Q 27001、JIS Q 15001 について、8.1.2 c2.(9)e として確認内容として追記し、従来の 8.1.2 c2.(9)e は示し、従来の 8.1.2 c2.(9)f として項番を繰り下げました。	d 財務諸表等に基づく経営の健全性 e 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 ・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2(日本公認会計士協会 IT7 号) ・AICPA SOC3 (SysTrust/WebTrustWebTrsuts)(日本公認会計士協会 IT2 号) 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 f 医療情報を保存する機器が設置されている場所(地域、国) g 受託事業者に対する国外法の適用可能性	d 財務諸表等に基づく経営の健全性 e JIS 15001、JIS Q 27001 の認証の有無 f 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 ・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2(日本公認会計士協会 IT7 号) ・AICPA SOC3 (SysTrust/WebTrustWebTrsuts)(日本公認会計士協会 IT2 号) 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 g 医療情報を保存する機器が設置されている場所(地域、国) h 受託事業者に対する国外法の適用可能性
83	8.4.2	・「8.4.2. 外部保存契約終了時の処理について」は 6 章～9 章の中で、他の章への参照を求めるケースを除き、唯一 C 項・D 項が存在せず、最低限実施すべき事項と推奨される事項の区分が不明確である。よって、B 項の内容に基づき、C 項・D 項を明確に定義すべきと思われる。これらを定義しない場合は、少なくとも、B 項(要求事項の解説及び原則的な対策方針)のみを記載し、具体的な事項を定義しない理由について明確に補足すべきと思われる。(C 項・D 項に記載がないため、実施する必要がないと勘違いするリスクがあるため)	参考意見として承りました。		
84	6.10	・「6.10. 災害、サイバー攻撃等の非常時の対応」-「(4) 非常時に備えたセキュリティ体制の整備」-B 項(p80)では、一定以上の医療機関等には『情報セキュリティ責任者(CISO)等の設置や、緊急対応体制(CSIRT 等)を整備するなどが強く求められる』旨が記載されている。一方で『強く求められる』要件であるにもかかわらず、本内容は C 項、あるいは D 項の要求事項として定義されていない。本 GL で『強く』という副詞をもって強調される要件(これを除くと 6 章以降では2つある)は全て C 項・D 項に何らかの観点で含まれている。そのため、CISO の設置や CSIRT の整備について 6.10 章の C 項への追加(または D 項の新設)、あるいは B 項の記載(『強く求められる』という表現)を見直すことが必要と思われる。(強く求めているにも関わらず最低限/推奨ガイドラインのいずれにも含まれておらず、該当要件がどのような位置付けなのか不明確であるため)	参考意見として承りました。		
85	全般	・30ページの最下行「漏れが無く」と、51ページの最下行から上に4行目「漏れない」とは、どちらかに字句を統一したほうが良いともいます。	ご指摘を踏まえて対応させていただきます。	本ガイドラインの要求に漏れが無く適合していることの確認が必要である。 第三者に漏れないように	本ガイドラインの要求に漏れなく 適合していることの確認が必要である。 第三者に漏れがないように P.31,51 を修正

整理番号	章	意見	考え方	修正内容	
				原案	修正案
86	4	・21ページの4行目「刑法」の法律番号を記載したほうが良いと思います。	ご指摘を踏まえて対応させていただきます。	刑法	刑法（明治40年法律第 45 号）
87	4.4.2 6.10	・26ページの23行目「いうまでも」と、72ページの14行目「言うまでも」とは、どちらかに字句を統一したほうが良いと思います。	ご指摘を踏まえて対応させていただきます。	言うまでも	いうまでも
88	6	・39ページの2行目「行政機関個人情報保護法」、3行目「独立行政法人等個人情報保護法」は法律名の略称の定義を記載したほうが良いと思います。3ページの25行目の「個人情報保護法」の例と同様に。	ご指摘を踏まえて対応させていただきます。	行政機関個人情報保護法 独立行政法人等個人情報保護法	行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号） 独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）
89	8.1.2	【該当箇所】 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 【修文案】 行政機関等が開設したデータセンター等に保存する場合は「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「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 【理由】 本文で加えられた第三者認証や外部監査は、政府情報システムの業務系クラウドサービスにおいて推奨されるレベル（安全管理ガイドライン第5版では「行政機関等が開設したデータセンター等に保存する場合」に記載）のものであると思われる。 「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」参照。	ご指摘いただいたものは、あくまでも参考文書として引用する趣旨ですので、原案の通りとさせていただきます。		
90	6.5	6.5. 技術的安全対策 ・「二要素認証」について，「マルチモーダル生体認証」は二要素に該当するかどうか明記していただきたいです。 ・新型コロナウイルス感染症のクラスターが発生した医療機関において，情報端末を経由して感染拡大した可能性があるとの報告があったので，情報端末の衛生管理についても規定をお願いします。感染症対策に関するガイドライン等に規定が別にあるのでしたら，そちらを明示することでも良いと思います。 ・情報端末の管理状況について定期的な端末の存在有無確認等を明示すべきではないでしょうか。医療機関外への持ち出しについては 6.9 で書かれているが，機関内の持ち出しもあり得る（ナースステーションから病室，会議室，医局等）ので，端末管理状況の把握は必要だと思います。	参考意見として承りました。		
91	6.7	6.7. 情報の破棄 ・「C. 最低限のガイドライン」の 2.と 3.の末尾に「～ことを確認すること。」とありますが，誰がというのを明示していただきたいです。最終的には病院管理者でしょうけど，CISO，安全管理責任者あるいは運用担当者による確認で良いかということになると思います。またその確認業務を外部業者に委託する場合においても基準があるとありがたいです。	本ガイドラインは医療機関等向けであることから、基本的には医療機関等における情報システム管理責任者等における実施事項を定めるものです。		
92	6.10	6.10. 災害、サイバー攻撃等の非常時の対応 ・CISO は1医療機関ごとに 1 人の設置が必要か，1法人で1人で十分かいずれでしょうか？	ご指摘の内容は個々のシステムや情報の取扱い状況によって異なるので、一意に定めることは困難であると解されます。具体的な状況を踏まえて判断していただくことを想定しております。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
93	1	該当箇所：1章の該当箇所：5 章では、新たに加わった厚生労働省標準規格や JAHIS 標準規約等を追記した。改版履歴の該当箇所：5 章では、厚生労働省標準規格や JAHIS 標準規約等を追加し、所要の改定を行った。修文案：1章の修正箇所：5 章では、新たに加わった厚生労働省標準規格や一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という）の標準規約等を追記した。改版履歴の修正箇所：5 章では、厚生労働省標準規格や JAHIS の標準規約等を追加し、所要の改定を行った。理由：JAHIS が初出の箇所に正式名称を追加すべきと考えます。また、可能であれば改訂履歴についても「の」を追加頂きたい。	ご指摘の箇所は、改定履歴であり、本文ではございませんので、参考意見として承りました。なお本文での初出では、ご指摘の団体名を示しております。		
94	4.3	該当箇所： 4.3.(1).(b).②の該当箇所： ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン(a)①に沿った考え方の整理が必要である。 修文案： 4.3.(1).(b).②の修正箇所： ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、(a)①に沿った考え方の整理が必要である。 理由： 参照先が合っていないと思われます。赤字の部分を削除すると違和感のない文章になります。	誤植ですので、ご指摘の通りの対応とさせていただきます。	ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン(a)①に沿った考え方の整理が必要である。	ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、(a)①に沿った考え方の整理が必要である。
95	6.2	該当箇所： なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集することが重要である。その際には、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド Ver3.0a」で示されているチェックリストが参考になる。 『製造業者による医療情報セキュリティ開示書』ガイド Ver3.0a」は以下の URL から取得できる。 修文案： なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集することが重要である。その際には、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」で示されているチェックリストが参考になる。 「『製造業者による医療情報セキュリティ開示書』ガイド」は以下の URL から取得できる。 理由： JAHIS の『製造業者による医療情報セキュリティ開示書』ガイドは本ガイドラインの発行に対応して最新版を出版予定です。Version を固定せず、常に最新版を参照することが望ましいため、バージョンを削除した方が良いと考えます。	ご指摘を踏まえてバージョンについての記載は削除いたします。	なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集することが重要である。その際には、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド Ver3.0a」で示されているチェックリストが参考になる。 『製造業者による医療情報セキュリティ開示書』ガイド Ver3.0a」は以下の URL から取得できる。	なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集することが重要である。その際には、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」で示されているチェックリストが参考になる。 「『製造業者による医療情報セキュリティ開示書』ガイド」は以下の URL から取得できる。 ※8.1.2 B 1. ②も同様
96	6.2	該当箇所： 医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集すること。例えば、「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」（総務省・経済産業省 令和 2 年 8 月 21 日）における「サービス仕様適合開示書」を利用することが考えられる。	ご指摘の箇所は、例示として参考文献を示す趣旨であり、全ての参考文献を示す趣旨ではありませんので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		修文案: 医療情報システムのベンダ及びサービス事業者から技術的対策等の情報を収集すること。例えば、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」又は「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」(総務省・経済産業省 令和 2 年 8 月 21 日)における「サービス仕様適合開示書」を利用することが考えられる。 理由: 要求事項においてはシステム提供のベンダと、サービス提供者のサービサーとを一緒に記載していますが、例示がサービス事業者に向けた例のみとなっていますので、JAHIS 標準を例に追加しました。修文案での JAHIS 標準を C 項の例に追加することに問題がある場合は、「サービス仕様適合開示書」がサービス事業者向けでシステムベンダ向けでないことを明記が必要です。			
97	6.5	該当箇所:なお、米国国立標準技術研究所(以下、「NIST」)から 2017 年 6 月に公表された「SP 800-63-3(Electronic Authentication Guideline(電子的アイデンティに関するガイドライン))第 3 版」においては、修文案:なお、米国国立標準技術研究所(以下、「NIST」)から 2017 年 6 月に公表された「SP 800-63-3(Digital Identity Guidelines(デジタルアイデンティに関するガイドライン))第 3 版」においては、理由:SP 800-63-3 は正式版で"Digital Identity Guidelines"となっています。和名もそれに合わせて修正が必要と思われます。	ご指摘を踏まえて対応させていただきます。	SP 800-63-3(Electronic Authentication Guideline(電子的アイデンティに関するガイドライン))第 3 版	SP 800-63-3(Digital Authentication Guideline(デジタルアイデンティに関するガイドライン))第 3 版
98	8.1	該当箇所: 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 修文案: 行政機関等が開設したデータセンター等に保存する場合は「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「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。 理由: 本要件は、政府情報システムの業務系クラウドサービスにおいて推奨されるレベル(安全管理ガイドライン第5版では② 行政機関等が開設したデータセンター等に保存する場合に記載)のものであるため、対象を限定すべきです。「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」参照。	ご指摘いただいたものは、あくまでも参考文書として引用する趣旨ですので、原案の通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
99	全般	意見その1 1. はじめに 「医療情報システムの安全管理に関するガイドライン第 5.1 版」（以下「本ガイドライン」といいます）において、厚生労働省がクラウドサービスの医療現場での普及への対応を明示いただいたことを歓迎いたします。 クラウド利用に関し、弊社は 2018 年に各府省情報化統括責任者（CIO）連絡会議が決定した「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」を強く支持いたします。 同文書は、政府機関情報システムにおけるクラウドサービスの利用に関する有益な指針を提供しています。 また、AWS は、CIO 連絡会議が、クラウドサービス固有のセキュリティ、機能、サポート、費用対効果を認め、クラウドサービスの採用を第一の選択肢として検討するよう機関に促す「クラウド・バイ・デフォルト原則」を策定したことを支持しています（同原則は、2019 年後半に閣議決定された「デジタル・ガバメント実行計画」でも示されています）。「クラウド・バイ・デフォルト原則」の考え方は、今後官民を問わず医療に従事する関係者の皆様に浸透していくものと期待いたします。そのうえで、医療に携わるクラウドサービス利用者は、「責任共有モデル」の下、個人情報やその他の関連する情報を保護し、クラウドサービス提供者とどのように連携するか深く理解し検討していく必要があると考えます。本ガイドラインは、その際の指針になるものと考えます。AWS は、クラウドサービスのリーディングカンパニーとしてのノウハウを共有し、将来にわたり、厚生労働省のガイドラインの策定等を支援していきます。	参考意見として承りました。		
100	4	2. 「4.　電子的な医療情報を扱う際の責任のあり方」について 本ガイドラインが、医療情報の処理における様々な類型を列挙し、事例に応じて責任分界の在り方を示し、医療機関等が委託者等との間で明確に合意すべき責任のあり方を示している点は高く評価できると考えます。 ただ、「4.2 委託と第三者提供における責任分界」において、本ガイドラインは「医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託（第三者委託）と第三者提供の 2 種類がある」ことを前提にしています。しかし、クラウドサービス提供事業者が提供するサービスはさまざまであり、医療機関等とクラウドサービス提供事業者との間に契約関係が存在しない場合、つまり委託にも第三者提供にも該当しない場合も考えられます。 例えば、AWS の責任共有モデル においては、「クラウド内」のデータ管理やアクセスコントロール、ファイアウォールの設定等については AWS の利用者様（AWS から見た顧客）が責任を持ちます（security in the cloud ともいいます）。この場合、その下のレイヤーのインフラ部分すなわち「クラウドの」のセキュリティについては AWS が責任を持つ、という合意がされております(security of the cloud ともいいます)。より具体的には、この共有モデルにおいては、AWS が、ホストオペレーションシステムと仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティに至るまでの要素を運用、管理及び制御します。AWS の顧客の皆様には、ゲストオペレーションシステム（更新とセキュリティパッチを含む）、その他の関連アプリケーションソフトウェア及び AWS が提供するセキュリティグループファイアウオールの設定に対する責任と管理を担っていただきます。この責任共有モデルによって柔軟性が得られ顧客の皆様がデプロイを統制できます。このような責任共有モデルは、クラウドを広く利用していただくために合理的に設計されており、実務で広く通用しているものです 。そして、このようなモデルの場合、AWS ユーザーと医療機関等との間では委託契約が存在しますが、医療機関等と AWS との間には委託契約関係は存在しません。もちろんクラウドサービスは多様ですので、AWS の責任共有モデルがすべてのクラウドサービスに適用されるわけではありませんが、逆に、「医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託と第三者提供の2種類がある」とすることも正確ではありません。 （その2に続きます）	ご指摘の点ですが、基本的にはサービス利用している以上、医療機関等から見て、利用サービスとの関係で何らかの契約関係（サプライチェーンによる形を含む）が発生していると考えられます。ご指摘の箇所でいえば、①のケースに当たるかと存じますが、。例えば以降は、一般的にはサービス提供ベンダ（SaaS）と PaaS や IasS などとの間で契約されており、医療機関等から見ると、再委託または類似の関係にあると整理されることが想定されます。なおこの場合でも、データの提供に関する取決めによっては、個人情報保護法上の第三者提供に該当する可能性ありうるかと存じます。		
101	4	意見その2医療機関等と同機関等より委託を受ける事業者との間の契約形態は、実務上、多種多様であり、この多様性から、契約当事者間の契約形態と合意内容に応じて、ひとくくりにできない当事者間のさまざまな義務や責任が発生します。事業者が自らの義務と責任を取捨選択し、それをリスクマネジメントのプロセスに落とし込んで医療機関等との間で合意を形成することを、本ガイドラインでも尊	ご指摘の点に関し、クラウドサービス事業者と医療機関等との関係も多種多様（医療機関等が IaaS 事業者と直接契約して、そのうえで構築をベンダーに依頼する等）であることから、クラウドベンダーであ		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		重すべきと考えます。より具体的には、「対象事業者が、いわゆる責任共有モデルのもとでクラウドリソースを調達する場合には、当該クラウドリソースを提供するクラウドサービス提供事業者と医療機関等との間には委託契約関係が存在せず、よって当該クラウドサービス提供事業者は本ガイドラインの対象にあたらない場合があること」を、明記いただくべきと考えます。 上記のような考え方は、個人情報保護法の解釈とも整合します。個人情報保護委員会が公表している「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関する Q&A（平成 29 年 2 月 16 日、同 30 年 7 月 20 日更新 ）の「Q5-33」(同 34 ページ)には、「個人情報取扱事業者が、個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用している場合、個人データを第三者に提供したものとして、『本人の同意』（法第 23 条第 1 項柱書）を得る必要がありますか」との問いに対し、次のように答えています。すなわち、「当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、『本人の同意』を得る必要はありません」としており、その「クラウドサービス提供事業者が個人データを取り扱わない場合」とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合が考えられます」としています。当該部分は、一定の契約合意によって、クラウドベンダーが個人データの取扱いの委託を受けているのではなく、クラウドサービスを利用している事業者（AWS の場合でいえば弊社の顧客の事業者様）が、個人データの取扱い主体であることを明らかにしています。この解釈は、個人データの取扱いに限らなくとも、クラウド利用契約での合意により、クラウドサービス提供事業者は「クラウドのセキュリティ」(security of the cloud)について責任を負い、クラウドサービス利用者は「クラウド内のセキュリティ」(security in the cloud)について責任を負うものとしている場合に、当該クラウドサービス提供事業者は受託当事者ではない、とすることと整合します。 前記の明確化を行うことで、クラウドサービスの利用時の注意点について記載する「委託と第三者提供における責任分界」の記述が、より本ガイドラインの利用者に理解しやすくなると考えます。	ることを以て、一律に本ガイドラインの対象外とすることは難しいと考えられます。		
		3.　「8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」について 本ガイドラインが、外部保存を受託する機関の選定基準への対応について指針を示している点は評価できます。しかし AWS として次の点を指摘させていただきたいと考えます。	ご指摘の点に関しては、「「診療録等の保存を行う場所について」の一部改正について」において、外部保存を行う際には、「「医療情報システムの安全管理に関するガイドライン」、受託する民間事業者等においては、「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」、さらにASP・SaaSを利用する事業者の場合においては、「ASP・SaaSにおける情報セキュリティ対策ガイドライン」及び「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」が遵守されることが前提条件であること」が示されています。本ガイドラインでも8.1.2　C2（3）において、「総務省・経済産業省の定めた『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』を遵守していることを契約に含めることを求めております。よって原案通りとさせていただきます。		
102	8.1.2	(1)　まず「1.　外部保存を受託する事業者の選定基準」において、医療機関等は「総務省・経済産業省の定めた『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』の要求事項も満たす必要がある」としている点は、修正が必要と考えます。総務省・経済産業省の定める上記ガイドラインは、リスクベースのアプローチによる要求事項を定めています。よって、医療機関等向けの本ガイドライン（規範的アプローチを採用）とはアプローチが異なります。したがって、「医療機関等は、総務省・経済産業省の定めた『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』のリスクベースに基づくアプローチについても理解し、提供事業者とのコミュニケーションに務める必要がある」と修正することを推奨いたします。 （その3に続きます）			

整理番号	章	意見	考え方	修正内容	
				原案	修正案
103	8.1.2	（意見その3） (2)　次に「1. 外部保存を受託する事業者の選定基準」において、「外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、所管する行政機関の調査等に供するため、提出等を行う必要が生じうることから、これを円滑に実現できることが求められる。そのため外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められる」とある点については、適切でないと考えます。 AWS のようなクラウドサービスの場合には、利用者の方との合意によって、日本法を準拠法とし、日本法にしたがってサービスを規律することが可能です。加えて、医療情報を行政機関等の調査等に供する場合においては、データのオーナーシップを持つ者つまりデータをコントロールしている者に対し、国内法令にもとづき提出等を求めるべきであり、行政機関等が医療機関等に資料提出を命ずることが可能と考えられます。そうすると、医療機関等が国内法の検討に加え「これを阻害するような国外法の適用がないこと」まで確認する必要はないと考えられます。 よって、「外部保存されている医療情報は、」から「適切に判断した上で選定することが求められる」までの前記記述は、削除されることを推奨いたします。	ご指摘の箇所につきましては、国外法の適用可能性については、確認事項としております。これは、医療機関等が行政機関や司法機関等の求めに対して、円滑に資料を提供しえない、ないしは保護措置がとれなくなるリスクを勘案して、各医療機関の実態に即して、事業者の選定を求めるための確認事項として示すものです。特に海外事業者において、本国と日本の国内法から同時に責務を負う場合には、当該事業者の判断に委ねられることになることから、医療情報管理に対して、医療法上の責務を負う医療機関においては、そのリスクを確認して、外部保存の委託先を選定することを求める趣旨です。		
104	9.5	（対象箇所)9.5（補足） 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合　B. 考え方紙等の媒体で扱うことが著しく利便性を欠くためにスキャナ等で電子化するが、紙等の媒体の保存は継続して行う場合、電子化した情報はあくまでも参照情報であり、保存義務等の要件は課せられない。しかしながら、個人情報保護上の配慮は同等に行う必要があり、またスキャナ等による電子化の際に医療に関する業務等に差し支えない精度の確保も必要である。（中略）C. 最低限のガイドライン 1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。・診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンすること。これは紙媒体が別途保存されるものの、電子化情報に比べてアクセスの容易さは低下することは避けられず、場合によっては外部に保存されるかもしれない。従って、運用の利便性のためとはいえ、電子化情報は元の文書等の見読性を可能な限り保つことが求められるからである。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできる。・放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン 3.0 版（平成 27 年 4 月）」を公表しており、参考にされたい。・このほか心電図等の波形情報やポラロイド撮影した情報等　様々な対象が考えられるが、医療に関する業務等に差し支えない精度が必要であり、その点に十分配慮すること。・一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がない精度であること、及びスキャンの対象となった紙等の破損や汚れ等の状況も判定可能な範囲であることを念頭に行う必要がある。放射線フィルム等の医用画像情報をスキャンした情報は DICOM 等の適切な形式で保存すること。2. 管理者は、運用管理規程を定めて、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。3.　緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。4.　電子化後の元の紙媒体やフィルムの安全管理を行うこと（意見内容）ア）本 9.5 章における原本は、電子化された情報であるのか、紙媒体であるのかが明確でない。2 つの原本が存在するのも法律上も実用上も違和感があると思いますので、明確にされたほうがよいと思いますイ）「運用の利便性のためとはいえ、電子化情報は元の文書等の見読性を可能な限り保つことが求められるからである。」との記載から、原本は紙媒体と思われます。この場合には、最低限のガイドラインの 「4 電子化後の元の紙媒体やフィルムの安全管理を行うこと」 の中の　電子化後の元の紙媒体の記述は不適と思われます。その理由は、紙媒体は電子化しても、電子化しなくても原本であるからです。従いまして、電子化作業による盗難紛失の脅威が増加することも配慮して	ご指摘の箇所につきましては、紙媒体等の原本に対して、電子化を行った場合の原本管理に関する要求事項を定めたものですので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		修文案としましては、4 原本とする紙媒体やフィルムは、電子化作業前後の安全管理を行うことと考えます。以上よろしくお願いいたします			
105	3.1	該当箇所 ～、e-文書法省令、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第2号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下「施行通知」という。）で定められた～ 意見内容 通知名は”「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」の一部改正について”であり、通知番号は”医政発 0331 第 30 号／薬生発 0331 第 10 号／保発 0331 第 26 号／政社発 0331 第 1 号”ではないか？元の通知名で記載するのであれば、平成 28 年は改正通知である旨を示してはどうか？ 理由 通知番号間違い、並びに通知名を正確に示すため	ご指摘を踏まえて対応させていただきます。	e-文書法省令、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第2号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下「施行通知」という。）で定められた	e-文書法省令、「「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」の一部改正について」（平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 10 号・保発 0331 第 26 号・政社発 0331 第 1 号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下「施行通知」という。）で定められた
106	3.1	該当箇所 なお、次に掲げる文書等のうち、「※」を付した処方せんについては、施行通知第二 2(4)の要件を充足する必要がある。 意見内容 施行通知第二 2(4)の要件を注釈で良いので、記載したほうが良いのではないか？ 理由 ガイドラインとしての読みやすさのため 備考 (4) 処方せんの取扱い 処方せんを電磁的記録により保存、作成及び交付等する場合の取扱いについては「電子処方せんの運用ガイドラインの策定について」(平成 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第 2 号厚生労働省医政局長、医薬・生活衛生局長、保険局長及び政策統括官(社会保障担当)連名通知。以下「運用ガイドライン」という。)において、運用に当たっての考え方や要件を示しているので、これに沿った運用を行うこと。なお、交付及び保存について特に留意すべき点は次のとおりであること。 ① 処方せんの電磁的記録による交付 運用ガイドラインに沿って、処方せんを電磁的記録により交付する場合には、交付の相手方である患者において、当該記録を出力することにより書面の作成ができるようにすることを要しないこと。 ② 紙媒体で交付された処方せんの保存 医師等から紙媒体で交付された処方せんを薬局でスキャナ等により電子化して保存することについては、(3)の要件のもとに認められるものであること。 なお、院内における処方せん(病院(診療所)に置かれる調剤所に対する指示書を含む。)の保存については、(3)の要件のもとにスキャナ等により電子化して保存することについて認められるものであること。	ご指摘につきましては、ガイドラインで参考文書を示しておりますので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
107	4.1	該当箇所医療情報システムの機能や運用方法が、その取扱いに関する基準を満たしていることを、患者等に説明できるようにする責任である。意見内容表現がおかしいのではないか。”医療機関等の管理者が、医療情報システムの機能や運用方法について、その取扱いに関する基準を満たしていることを、患者等に説明できるようにする責任である。”などではないか？理由ガイドラインの読みやすさのため	ご指摘を踏まえ、「医療情報システムの機能や運用方法等の取扱いに関する基準を満たしていることを患者等に説明できるようにする責任である。」とさせていただきます。	医療情報システムの機能や運用方法が、その取扱いに関する基準を満たしていることを患者等に説明できるようにする責任である。	医療情報システムの機能や運用方法等の取扱いに関する基準を満たしていることを、患者等に説明できるようにする責任である。
108	4.2.2.	該当箇所 ～、情報処理関連事業者と医療機関等の提供元間で、～ 意見内容 表現がおかしいのではないか。 ”～、情報処理関連事業者と提供元である医療機関等との間で、” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえ、「情報処理関連事業者と医療機関等の間で」とさせていただきます。	情報処理関連事業者と医療機関等の提供元間で	情報処理関連事業者と医療機関等の間で
109	4.3	該当箇所 ただし、情報処理関連事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン(a)①に沿った考え方の整理が必要である。 意見内容 参照先がおかしいのではないか？ 本項で述べている責任分界点に対する整理を述べている箇所が無いように見受けられる。 理由 参照間違いと思われるため	誤植ですので、「一般社団法人保健医療福祉情報システム工業会（以下「JAHIS」という） 基本データセット適用ガイドライン」を削除させていただきます。		
110	4.3	該当箇所 なお、リモートメンテナンスも含めた保守の考え方については、6.8 を参照されたい。 意見内容 記述ミス ”なお、リモートメンテナンスも含めた保守の考え方については、6.8 章を参照されたい。” 理由 他の修正と平仄を合わせるため	ご指摘を踏まえて対応させていただきます。	なお、リモートメンテナンスも含めた保守の考え方については、6.8 を参照されたい。	なお、リモートメンテナンスも含めた保守の考え方については、6.8 章を参照されたい。
111	4.3	該当箇所 なお、治験のように、～ 意見内容 医学研究の場合も例として記載してはどうか？ 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、例として示す趣旨であり、網羅的に例を示す趣旨ではありませんので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
112	4.3	該当箇所 (4) オンライン外部保存を委託する場合 意見内容 オンライン外部保存という用語で解釈がぶれることが想定されるため、下記のように修正してはどうか？ (4) オンラインによる外部保存を委託する場合 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて、「オンライン外部保存」について、用語集で示させていただきました。		
113	4.3	該当箇所 ～、医療機関等が説明責任を果たすための資料や説明の提供を受託する事業者との契約で定め、～ 意見内容 これ以降、受託事業者と略しているため、初出として、”～受託する事業者（以降、受託事業者という）との契約で定め、～”としてはどうか 理由 ガイドラインの読みやすさのため	受託事業者については、一般的な用語として使用しておりますので、原案通りとさせていただきます。		
114	4.3	該当箇所下図の②の場合は、～意見内容下図を正しい図表番号を参照するようにすべき（図 4-3-1）理由ガイドラインの読みやすさのため	ご指摘を踏まえて、対応いたします。	下図の②の場合は、	図 4-3-1 の②の場合は、～ P.30,82,83,85,88,89,90 を修正
115	4.3	該当箇所 下図の②の場合は、～ 意見内容 ①の場合の説明を加えるべきではないか？ 理由 ガイドラインの読みやすさのため	ご指摘の箇所は、特に②のケースに着目して説明する趣旨ですので、原案通りとさせていただきます。		
116	4.3	該当箇所 法令で定められている場合等の特別な事情により、情報処理関連事業者に暗号化されていない医療情報が送信される場合は、～ 意見内容 ”情報処理関連事業者”について、用語の定義を行うか、初出で説明を行うように記載をしてはどうか？ 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて、用語集で対応いたしました。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
117	4.3	該当箇所 ～、情報処理関連事業者又はネットワークにおいて盗聴の脅威に対する対策を施す必要がある。 意見内容 表現を正確に記載する必要があるのではないか？ ”情報処理関連事業者及び利用するネットワークを提供する事業者において盗聴の脅威に対する対策を施す必要がある。” 理由 対象を明確にするため	ご指摘を踏まえて、「情報処理関連事業者及びるネットワーク通信事業者等において盗聴の脅威に対する対策を施す必要がある」とさせていただきます。	情報処理関連事業者又はネットワークにおいて盗聴の脅威に対する対策を施す必要がある。	情報処理関連事業者及びネットワーク事業者等において盗聴の脅威に対する対策を施す必要がある
118	4.4	該当箇所 ～システム要件と運用管理規程を選択する必要がある。この選択は、安全性に対する脅威、～ 意見内容 下記の表現の方が適切ではないか？ ”～システム要件と運用管理規程について判断し決定する必要がある。この決定は、安全性に対する脅威、～” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて「システム要件と運用管理規程について決定する必要がある。」させていただきます。	システム要件と運用管理規程を選択する必要がある。この選択は、安全性に対する脅威、	システム要件と運用管理規程について決定する必要がある。この決定は、安全性に対する脅威
119	4.3	該当箇所 「例えば」以下 意見内容 「例えば、以下」を以下のように追加修正する。 「医療情報を取り扱う情報システム・サービスの提供事業者における安全 管理ガイドライン」（総務省・経済産業省　令和 2　年 8　月 21　日）における「サービス仕様適合開示書」 あるいは 「JAHIS　標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド Ver3.0a」で示されている「製造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」を利用することが考えられる。 理由 「製造業者による医療情報セキュリティ開示書」は「6.2 章 B 考え方」でリスク分析の技術的対策等の情報の収集先として引用されている。 総務省・経産省のガイドラインを C 項で引用するのであれば「6.2 章 B にも併記すべきである。 「両省提供事業者ガイドライン」の FAQ1.1 ではガイドラインは「医療機関等が、その医療機関等内において、対象事業者に委託等することなく、自ら医療情報を取り扱っている医療情報システム場合は対象範囲外」となっているので、「両省のガイドラインによる開示書」の適用範囲は厚労省ガイドラインの範囲の中で限定されていることになり、工業会規格の方が全体をカバーしている。	参考意見として承りました。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
120	6.2	該当箇所 上記 1 から 6 の結果を系統的に文書化して管理すること。 意見内容 表現がおかしいのではないか？ ”系統的”→”体系的”？”系統別”？ 理由 誤植？	参考意見として承りました。		
121	6.5	該当箇所～アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行うこと。～意見内容記述ミスではないか？”（アクセス権限）”→”（以降、アクセス権限という）”理由ガイドラインの読みやすさのため	ご指摘の箇所は、「アクセスできる診療録等の範囲」という記述の意義を示す趣旨で、（アクセス権限）としめしたものです。 原案通りとさせていただきます。		
122	6.5	該当箇所 電波を発する機器（携帯ゲーム機等）による電波干渉に留意すること。 意見内容 スマートフォンを例に加えてはどうか？ 理由 現状に合わせるため	ご指摘の部分は、「等」に含まれていると解しておりますので、原案通りとさせていただきます。		
123	6.6	該当箇所 （b） 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取り扱い、守秘義務を負う者 ～(c)に対する人的安全対策は、事務取扱委託業者の監督及び守秘義務契約として説明する。 意見内容 ”事務取扱委託業者”、”事務委託者”の標記の揺れがある。 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、事務委託者と事務取扱委託業者は異なる趣旨で使用しております。 ご指摘を踏まえて「事務取扱委託業者」は「事務取扱受託業者」といたします。	事務取扱委託業者	事務取扱受託業者 P.63,64 を修正
124	6.8	該当箇所 メンテナンスを実施するためにサーバに保守会社の作業員（保守要員）が～ 意見内容 記述ミスではないか？ ”（保守要員）”→”（以降、保守要員という）” 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、保守要員は一般的な用語として用いておりますので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
125	6.11	該当箇所 ～現在のネットワーク機器に INS-VPN 変換アダプタを装着する方法等や、～ 意見内容 INS-VPN 変換アダプタは一般的な呼称なのか？下記のような表現がいいのではないか？ ”INS から VPN に変換するアダプタを～” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて、「INS から IP-VPN に変換するアダプタ」とさせていただきます。	INS-VPN 変換アダプタ	INS から IP-VPN に変換するアダプタ
126	6.11	該当箇所 ～患者との関係で責任分界についても取り決めておくことが求められる 意見内容 句点が抜けている。 ”～患者との関係で責任分界についても取り決めておくことが求められる。” 理由 誤植	ご指摘を踏まえて対応させていただきます。	～患者との関係で責任分界についても取り決めておくことが求められる	～患者との関係で責任分界についても取り決めておくことが求められる。
127	6.11	該当箇所 ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざん又は中間者攻撃等を防止する対策を実施すること。 意見内容 表現を正確に記載する必要があるのではないか？ ”ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。” 理由 対象を明確にするため	ご指摘を踏まえて対応させていただきます。	ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざん又は中間者攻撃等を防止する対策を実施すること。	ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。
128	8.1.2	該当箇所「4. 電子的な医療情報を扱う際の責任のあり方」及び「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。意見内容記述ミス”4 章及び 6.11 章と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。”理由他の修正と平仄を合わせるため	ご指摘を踏まえて対応させていただきます。	「4. 電子的な医療情報を扱う際の責任のあり方」及び「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。	4 章及び 6.11 章と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。
129	8.1.2	該当箇所 外部保存の技術的な方法としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。 意見内容 内容が技術的な方法となっていない。修正するのであれば、下記ではないか？ ”外部保存の方法に対し、技術で求める要件としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを技術で担保するようことを事業者に求めることも考えられる。” 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、患者情報を医療機関等のみがデータ内容を閲覧できることを担保すること外部保存先の事業者に求める趣旨であり、技術的な措置を講じることを求める趣旨です。原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
130	8.1.2	該当箇所 ～担保することも考えられる。 さらに、外部保存を受託する事業者に保存される～ 意見内容 ”さらに”の一段落は例示の一つであるため、改行をしない方がいいのではないか？ 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、例を具体的な内容として示す趣旨ですので、原案通りとさせていただきます。		
131	8.1.2	該当箇所 具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられる。 意見内容 前後とのつながりがおかしいため、下記のように修正してはどうか？ (改行をせずに)”具体的には、外部保存を受託する事業者において、「関係者外から保存する情報にアクセスできないように制御を行う」、「保存する情報に対して暗号化を行う」、「保存する情報を分散保管する」方法が考えられる。” 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、例を具体的な内容として示す趣旨ですので、原案通りとさせていただきます。		
132	8.1.2	該当箇所 ”この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならない。”以降 意見内容 具体的方法である「暗号化を行う」に関する事項のみになっているため、その他の方法に対する記載を加えてはどうか？ 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、例を具体的な内容として示す趣旨ですので、原案通りとさせていただきます。		
133	8.1.2	該当箇所 ～、あくまで医療機関等同士の同意で実施されなくてはならず、当然、個人情報保護法に則り、患者の同意も得た上で実施する必要がある。 意見内容 医療機関の同意は表現としておかしいのではないか？ ”～、あくまで医療機関等同士の同意で実施されなくてはならず、～” →”～、あくまで医療機関等同士の合意の下で実施されなくてはならず、～” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて対応させていただきます。	あくまで医療機関等同士の同意	あくまで医療機関等同士の合意

整理番号	章	意見	考え方	修正内容	
				原案	修正案
134	8.1.2	該当箇所 ～、医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等して、～ 意見内容 文章が分かりにくいのではないか？ ”～、医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等して、～” →”～、医療機関等による求めに応じる形、若しくは患者自身の情報を提供することに対する同意を医療機関等と行った上での求めに応じる形で、適切な権限を設定する等して、～” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて、「医療機関等又は医療機関等に対して同意した患者の求めに応じてとさせていただきます。	医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて	医療機関等又は医療機関等に対して同意した患者の求めに応じて
135	8.1.2	該当箇所病院や診療所の内部で診療録等を保存させること。意見内容文章が分かりにくいのではないか？”病院や診療所の内部で診療録等を保存させること。”→”病院や診療所の内部に診療録等を保存すること。”理由ガイドラインの読みやすさのため	ご指摘を踏まえて対応させていただきます。	病院や診療所の内部で診療録等を保存させること	病院や診療所の内部に診療録等を保存すること。
136	8.1.2	該当箇所 匿名化した情報であっても、匿名化の妥当性の検証や、院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。 意見内容 並列の関係にないものが”や”でつながっている。下記のように修正するべきではないか？ ”匿名化した情報であっても、匿名化の妥当性の検証を行う、および院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。” 理由 ガイドラインの読みやすさのため	ご指摘を踏まえて対応させていただきます。	匿名化した情報であっても、匿名化の妥当性の検証や、院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。	匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。
137	8.1.2	該当箇所 保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存を受託する事業者に適切なアクセス権を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮よう求めること。 意見内容 文が分かりにくい。しかも病院、診療所、医療法人等が適切に管理する場所の話の箇所であるため、下記のように修正してはどうか？ →”保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存を受託する医療機関等に対して適切なアクセス権の設定を依頼し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないような配慮を求めること。” 理由 ガイドラインの読みやすさのため	本ガイドラインでは患者を名宛人とするのではなく、医療機関等を名宛人として要求事項等を示しておりますので、原案通りとさせていただきます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
138	8.1.2	該当箇所 なお保守に関しては、6.8 章を遵守すること。 意見内容 医療機関等が事業者に求めることではないか？ →”なお保守に関しては、6.8 章を遵守させること。” 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、6.8 章には医療機関が自ら実施することと事業者が実施することが含まれており、事業者が実施すべきことについては、「させる」という表現を用いております。原案通りとさせていただきます。		
139	8.1.2	該当箇所全体意見内容下線部の追加「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」の「第三者認証等の取得に係る要件」及び、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。・プライバシーマーク認定・ISMS 認証パブリック・クラウドに関しては以下も推奨される。・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク・米国 FedRAMP・AICPA SOC2（日本公認会計士協会 IT7 号）・AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2 号）上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。・システム監査技術者・Certified Information Systems Auditor ISACA 認定理由本要求事項の目的は「技術及び運用管理能力の有無の確認」であるが「下記のいずれかの認証等により」となっているので、いづれかの認証を取っていることを要求していることになる。一方、C.2.(3)では「 総務省・経済産業省の定めた「安全管理ガイドライン」を遵守することを契約等で明確に定めること」が必須となっていて、その P20 4.4. 第三者認証等の取得に係る要件」では、「プライバシーマーク認定または ISMS 認証を取得すること。」が必須となっている。類似した認証を2種類取ることを要求され企業等には負担になり、クラウドシステムの発展を推進することを阻害する。「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 4.2」ではプライベイトクラウドに関しては****が推奨される」となっている。これらのガイドラインと今回のガイドラインの基本方針との整合性をとったものとして、左記の意見内容を提案させて頂きました。備考なお、8.1.2.D.1. において、「個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークや ISMS 認定等の第三者による認定を取得している事業者を選定すること。」として、推奨事項として同様な記述があり、左記の C 項としての必須項目と重なってしまいますが、この項は、「病院、診療所、医療法人等が適切に管理する場所に保存する場合」も含めた要求事故と解釈すれば、齟齬はないと考えます。	本項は確認事項であり、必須事項ではありません。なおご指摘を踏まえて、JIS Q 27001、JIS Q 15001 について、8.1.2 c2.(9)e として確認内容として追記し、従来の 8.1.2 c2.(9)e は示し、従来の 8.1.2 c2.(9)f として項番を繰り下げました。	d 財務諸表等に基づく経営の健全性 e 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク・米国 FedRAMP・AICPA SOC2（日本公認会計士協会 IT7 号）・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。・システム監査技術者・Certified Information Systems Auditor ISACA 認定 f 医療情報を保存する機器が設置されている場所(地域、国)g 受託事業者に対する国外法の適用可能性	d 財務諸表等に基づく経営の健全性 e JIS 15001、JIS Q 27001 の認証の有無 f 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無。・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク・米国 FedRAMP・AICPA SOC2（日本公認会計士協会 IT7 号）・AICPA SOC3（SysTrust/WebTrustWebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力をの有無を確認すること。・システム監査技術者・Certified Information Systems Auditor ISACA 認定 g 医療情報を保存する機器が設置されている場所(地域、国)h 受託事業者に対する国外法の適用可能性
140	8.1.2	該当箇所 全般 意見内容 B.2.で記載した内容がそのまま記載されているため、文章がおかしい。きちんと検討していただきたい 理由 ※記載なし	参考意見として承りました。		
141	8.1.2	該当箇所 医療機関等の以外外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合では、～ 意見内容 誤植ではないか？ →”医療機関等以外の外部の事業者との契約に基づいて確保した安全な場所に保存する場合では、”	ご指摘を踏まえて対応させていただきます。	医療機関等の以外外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合

整理番号	章	意見	考え方	修正内容	
				原案	修正案
		理由 ガイドラインの読みやすさのため			
142	9.5	該当箇所 これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからである。 ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできる。 意見内容 電子化情報は分かりにくいのではないか？”電子化された情報”としたほうがいいのではないか？ 理由 ガイドラインの読みやすさのため	ご指摘の箇所につきましては、記載個所との関係で電子化情報という表現でも、誤解を与える恐れは少ないと考えられますので、原案通りとさせていただきます。		
143	6.5	意見その1 （該当箇所） (1)利用者の識別及び認証 二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、 令和9年度時点で稼働していることが想定される医療情報システムを今後導入 又は更新する場合、原則として二要素認証を採用することが求められる （意見） ア)原則として　という表現が曖昧なので、QA あるいは付則等で解説をご検討ください イ)ア)の点をふまえ、医療機関側の負担費用が大きい可能性がありますので、新規導入と更新での二要素認証の採用条件を変えてもらうほうが現実的であり、普及を促進すると思います	ア　ご指摘の箇所につきましては、QA で対応させていただきます。 イ　参考意見として承りました。		
144	6.5	意見その2（該当箇所）6.5 技術的安全対策（バイオメトリクスを利用する場合の留意点）（中略）これらのことを踏まえ、実際に採用することが想定される 2 要素二要素認証の方式として、下記の例が挙げられる。2 要素二要素認証の採用例　ユーザ ID とパスワード＋指紋認証　IC カードとパスワード　IC カードと静脈認証　等（意見）　例えばスマートフォン、タブレットに採用されている ID とパスワードと指紋認証の組み合わせはガイドラインで求めてられている二要素認証の方式に合致しているかご教示ください	ご指摘の方法については、具体的な方法にもよるため、二要素認証に該当するとは必ずしも判断できませんが、一般的な方法であれば、二要素認証となりうるものと解せられます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
145	6.11	意見その3 （該当箇所） 6.11　外部と個人情報を含む医療情報を交換する場合の安全管理 オープンなネットワークで接続されていする場合 「SSL/TLS 暗号設定ガイドライン 3.0.1 版」では 3 段階の設定基準が定められているところおり、医療情報システムで利用する場合は、そのうち最も安全性水準の高い「高セキュリティ型」の設定を反映することで SSL/TLS への攻撃リスクを低減する必要がある。なお、「高セキュリティ型」の設定の一つとして、利用可能なプロトコルバージョンを TLS1.3 以上に設定するが、システムやサービス等の対応上、これによることが難しい場合には、TLS1.2 に限定して設定する必要がある。 そのため、サーバ・クライアントともに TLS1.2 以上をサポートしていることが必須となることに注意されたい（TLS1.2、TLS1.3 のいずれかの利用に限定している場合には、それぞれのプロトコルをサポートしていることが求められる） （意見） 上記項番で規定の 「システムやサービス等の対応上、これによることが難しい場合には、TLS1.2 に限定して設定する必要がある。そのため、サーバ・クライアントともに TLS1.2 以上をサポートしていることが必須となることに注意されたい（TLS1.2、TLS1.3 のいずれかの利用に限定している場合には、それぞれ のプロトコルをサポートしていることが求められる）」においては、 例えば患者本人や介護士のスマートフォン等から電子処方箋サーバや地域連携協議会が開設する医療情報が格納されるサーバに患者の同意のもとにその患者の医療情報を閲覧する場合も該当しますか？ その場合には、クライアント側が旧型のスマートフォン（OS)である場合には TLS1.3 の設定が不可能なことも考えられ、電子処方箋や地域連携等の普及の障壁にもなると思いますので、二要素認証のように移行期間、緩和条件を設けていただけたほうがよいと思います 以上よろしくお願いします	ご指摘の箇所は、TLS1.3 を原則として求めるものの、例外的に TLS1.2 による対応も認めております。		
146	全般	この度、令和 2 年度診療報酬改定の概要(3/5 改訂版)の P25 に、「文書による患者の同意を要件としているものについて、電磁的記録によるものでも良いことを明確化する」との記述がございます。 本件について、診療報酬改定には記載があるものの、その詳細や具体策に関しての記載が無く、今回のガイドライン第 5.1 版においても、改めて明確に認める記述や具体的な運用方法の例等の記載について、ご検討頂くことは出来ませんでしょうか。 働き方改革が推進される昨今、スキャン業務の省力化に向けて、医療機関様からも電子サイン化を望む声が数多くあることや、昨今の新型コロナ感染防止の観点においても、医療機関様より紙の受け渡しによる感染リスク軽減が出来るとのご意見もあり、意見として提出を致します。ご検討の程、宜しくお願い致します。	本ガイドラインでは、法令で署名又は記名・押印が義務付けられた文書等については、6.12 章において定める電子署名によることとしています。これ以外のタブレットやスマートフォン上で行う手書きのサイン等の電磁的記録を含めた形が可能とする、法令で署名又は記名・押印が義務付けられた文書等はありません。また、本ガイドラインにおいて法令で署名又は記名・押印が義務付けられた文書等に関する扱いを記載することは混乱を生じさせるおそれがあるため、原案のままとさせて頂きます。		

整理番号	章	意見	考え方	修正内容	
				原案	修正案
147	6.11	医療情報システムの安全管理に関するガイドライン 第 5.1 版（案）s49520023802.pdf に3点コメントいたします。カッコ内は PDF ファイルの実ページ番号を表します。 ■コメント1 P87(PDF 項 95 ページ) 6.11. 外部と個人情報を含む医療情報を交換する場合の安全管理 B-2. 選択すべきネットワークのセキュリティの考え方 II オープンなネットワークで接続する場合 記載： 必要に応じて、ネットワークの分離（例えばメールシステムと医療情報システムの分離）や、これを踏まえた情報交換のルールに基づく管理を行うことが望ましい。 コメント： 「ネットワークの分離」について、その言葉の持つ印象から物理層での分離と解釈する医療機関が少なからずあると思います、またその場合、専用ネットワーク機器を2重で構築するなど、設備面で負担がかかるのみならず今後の情報化計画に影響する懸念があります。オンライン診療や 5G/IOT、ゼロトラスト(NIST-SP800-207)等の動きから、医療情報システムにおいてもクラウド化を検討する動きがあるため、上記記載は、例えば「医療情報システムを分割する場合は、例えば VLAN 分割しクラウドサービスの必要な通信をホワイトリスト許可するなどの対応が望ましい、実現においてはゼロトラスト(NIST SP800-207)などのリファレンスを参考にすること」などの具体的なアクションをイメージできる記載を検討いただけると幸いです。 なお医療機関と類似する点が多い地方自治体においても、ネットワーク分離によりインターネットが活用できない現状から、一部ガイドラインを見直しをする発表「自治体情報セキュリティ対策の見直しについて」を行っています。https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html	参考意見として承りました。		
148	4.3	■コメント2P30(PDF 項 38 ページ) 4.3. 例示による責任分界点の考え方の整理(4)オンライン外部保存を委託する場合コメント：マイクロソフトが提供するクラウドサービスは図 4-3-1 が示す、B 垂直連携ケースのケースが該当するものと考えています。図 4-3-1 が示す別途契約には、オンラインサービス条項や SLA などでサービスの規定を定めており、この形態はグローバルスタンダードなものとなっています。医療機関でのクラウド調達において、耐震基準や物理監査を要件に含めるケースも数多く確認していますが、これらはクラウドサービスの実態とあわないため、クラウドサービスを求める医療機関様であっても提供がかなわないケースもございます。このためクラウドサービスの実態にあわせる形で、ご配慮頂ければ助かります。	参考意見として承りました。		
149	8.1.2	■コメント3 P123(PDF 項 131 ページ) C. 最低限のガイドライン 2.医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合 記載： (8) 保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。 コメント： 法の適用を受けるのは通常は組織（例：クラウドサービス事業者）であり、「機器等が受ける」は記載が不足していると思います。この点ご確認お願いします。	ご指摘の点に関しては、医療機関等が行政機関等や司法機関等からの求めに応じて、証拠を提供する際に、これを円滑に行えるようにする観点から国内法の適用を受けることとしております。従って、機器等の実際の物理的な管理状況により、管理者や処分権限者など、対象となる者の範囲は異なるとことを想定しております。よって原案通りとさせていただきます。		