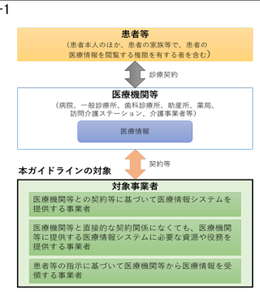
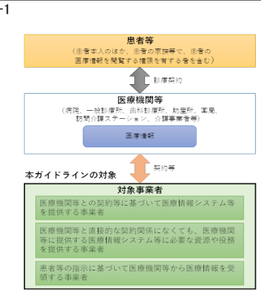
別紙2

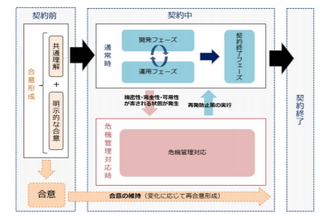
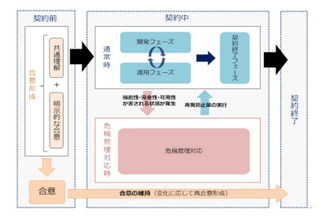
No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
1	個人	個人	01全般	0	全般	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。 例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。 具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。 （ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションオード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。 （イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。 （ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。 （エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。 具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。 （ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。 （イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。 （ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。	参考意見として承りました。		
2	個人	個人	01全般	0	全般	（続き） 具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。 （ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。 （イ）エッジコンピューティングでは、Web上における「URL（ユ ニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。 具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。 （ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。 （イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます	参考意見として承りました。		
3	一般社団法人 日本画像医療システム工業会	団体	01全般	0	全般	PDFにしおりをつけてくれたことは、参照する上で非常に助かります。 付録1は、MSWordのテンプレート書式 （dotx形式）、付録2はExcel形式で提供されると各事業者はそれらを有効に活用でき、さらに便利になると思われます。	閲覧性が保たれているPDFでの公開となります。		
4	一般社団法人 日本画像医療システム工業会	団体	01全般	0	全般	提供事業者が参考すべきガイドラインが、従来は総務省2ガイドライン、経済産業省1ガイドラインが、総務省1ガイドラインになり、さらに、今回、総務省と経済産業省とのガイドラインが統合される。省をまたいだ統合版の作成で、関係者のご尽力に敬意を表します。提供事業者にとっては、よりよくなったと感じます。	賛同意見として承りました。		
5	個人	個人	02GL	0	全般	問題6 現在の新型コロナウイルスの場合のような非常事態の場合の対応策を策定すること 現在の新型コロナウイルスのように、委託先、その再委託先等の多くの従業員（派遣労働者を含む。）が出勤できない場合、サービスレベルを保証できない、サービス自体も提供できない場合もあります。対策を検討しておくべきであると存じます。	参考意見として承りました。		
6	キヤノンメディカルシステムズ株式会社	団体	02GL	0	全般	明瞭に見えるような書体にしてほしいです。 カラーになっている部分が特にぼやけて見難いです。 文字が小さいためで視認性が悪いです。	ご指摘を踏まえて修正いたします。		（画像を再度貼付）
7	個人	個人	02GL	0	全般	現在の新型コロナウイルスの場合のような非常事態の場合 現在の新型コロナウイルスのように、 委託先、その再委託先等の多くの従業員（派遣労働者を含む。）が出勤できない場合、 サービスレベルを保証できないおそれ、サービス自体も提供できないおそれもあります。 非常事態における対策を検討し、事前に委託先と協議し、 契約書における非常事態時についての行動、対応策、サービスレベル等の共通認識を得て、 定めておくことも必要ではないかと存じました。	参考意見として承りました。		
8	グーグル・クラウド・ジャパン合同会社	団体	02GL	0	全般	制度開始前に本制度関係文書の英語版をご提供頂きたく存じます。	現時点において、本ガイドラインの英語版の作成予定はございません。		
9	グーグル・クラウド・ジャパン合同会社	団体	02GL	0	全般	何故本ガイドラインが、リスク管理システムの構築の詳細に立ち入る必要があるのか不明である部分がございます。代わりに、本ガイドラインのポイントの大部分をカバーできると思われるISMS（情報セキュリティマネジメントシステム）の導入をご検討頂きたく存じます。また、本ガイドライン内には、特定のテクノロジーの使用を求める箇所が複数認められます。これは関連する企業（及び医療機関）のイノベーションと競争力を阻害すると思われ、彼らがから、より優れた技術を利用するインセンティブ（動機）を奪っているとも言え、結果的に日本の産業・医療の国際競争力が弱まることを懸念しています。特定の技術要件を求めるのではなく、それらを利用する「目的」と具体的な「目標」をご設定頂ければ幸いです。また、データセンターや機器の物理的な位置に関する言及も数多くございますが、クラウドコンピューティングの世界では、一つのサービスが複数のリージョン（地域）とデータセンターにまたがる数千の機器を経由して提供されることは普通であり、そのセキュリティは「場所」によって担保されるものでは有りません。よって規制により、データセンターやその設置場所が要求されることは、医療機関による最新のテクノロジーやクラウドサービスの採用を難しくすると考えております。	本ガイドラインは、「医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する」という方針に基づき、可能な限り一律の要求事項を排すよう努めていますが、医療情報システム特有の考慮事項として必要と考えられる個別の要求事項については、これを記述しているものです。また、ISMS認証等については、医療情報を取り扱う事業者としての最低限の適格性を医療機関等へ示す公的な第三者認証として位置づけております。また、医療情報及び当該情報に係る医療情報システムが国内法の執行の及ぶ範囲にあることを確実とすることは、法令で定められた医療機関等に対する義務や行政手続の履行を確保するために必要な措置です。		
10	個人	個人	02GL	0	全般	問題6（補正及び補足） 今般の新型コロナウイルスの場合のような非常事態の場合 　今般の新型コロナウイルスのように、委託先、その再委託先等の多くの従業員（有期雇用の社員、派遣労働者を含む。）が出勤できない場合、サービスレベルを保証できないおそれ、サービス自体も提供できないおそれもあります。非常事態における対策を検討し、事前に委託先と協議し、契約書における非常事態時についての行動、対応策、サービスレベル等の共通認識を得て、定めておくことも必要ではないかと存じました。感染症流行、地震、豪雨災害、津波、浸水被害、火山噴火、戦争等も考えられます。	参考意見として承りました。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
11	個人	個人	02GL	0	全般	そして、ISMS運用上のインシデント報告、一覧への記載を避けることには、次のような組織が不正を働くおそれのある動機の因子、正当化の因子等があるのではないかと存じます。これらは、もみ消したい理由でもあると存じます。 1　外部のISMS認証等の認証機関に障害等が多い組織であると判断されること 2　ISMS認証が取り消されると、発注者の信頼を得にくくなり、業者は、受注を得ることが難しくなるおそれがあること 3　情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント等が発生すると、問題の報告書、是正処置報告書等を作成し、それを確認する面倒な作業が発生し、責任者等の残業等の労働時間が増えてしまうこと 4　障害等が多い部門の管理職は、能力不足と判断され、異動、降格等の処分になるおそれがあること 出世コースから外れたり、引っ越しをしなければならなくなるおそれもございます。 5　システムが多く、それぞれが複雑すぎること、システム内部をすべて完璧に理解していないこと等の理由から、委託先、再委託先等のトップマネジメント、責任者等は、通報されても、理解ができず、判断できず、責任をもった適切な指示ができないので、報告されることを嫌がるおそれがあること もし委託先、再委託先等のトップマネジメント、責任者等が間違った指示を行った場合、その方々の責任問題になります。そのため、情報セキュリティの問題の報告が多いと、4のようになるおそれがあります。 6　発注者としても、発注者の情報セキュリティ責任者としても、体裁として、情報セキュリティの問題発生が少ない印象の方を好むこと 情報セキュリティの問題の多発によって、発注者として毎回毎回大事になり、心労がかさむことは、避けたいのではないかと存じます。委託先、再委託先等の内部で受託業務の情報セキュリティの問題、情報事故等を曖昧に処理、もみ消してしまえば、発注者は、責任を回避できます。 所謂「不正のトライアングル」(「機会」、「動機」、「正当化」)等も考慮し、情報セキュリティの不正発生防止についてもご検討のほどよろしくお願いいたします。	参考意見として承りました。		
12	個人	個人	02GL	0	全般	問題7 これら以外の公正な第三者の認証等として、セキュリティ管理に係る内部統制保証報告書」(当ガイドライン20ページ)についても、記載がございましたが、これまでの様々な件に関係して、下記の内部統制の限界についてもご検討とご留意のほど、よろしくお願いいたします。	参考意見として承りました。		
13	個人	個人	02GL	0	全般	問題8 組織の情報セキュリティの運用状態の経年劣化 組織的には、最初は、良い状態でも、年数が経過するにつれ、巧妙なもみ消し方を覚え、状態が悪くなっていくおそれもございますので、ご検討とご留意のほど、よろしくお願いいたします。	参考意見として承りました。		
14	個人	個人	02GL	0	全般	問題9 組織の情報セキュリティの教育が不十分である問題 委託先、その再委託先等のISMS認証、PMS認証等の取得の有無にかかわらず、情報セキュリティに関する社内教育があると思いますが、細かなISMS、PMS等に関する組織の内部規定については、しっかりと理解させる教育になっていないおそれもございます。通報されるべき情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント、情報事故等の定義、ISMS認証、PMS認証等の適用範囲等すらも教育せず、曖昧な理解を社内に浸透させれば、通報されるべき問題をもみ消せるおそれもございます。 以上、公衆衛生の向上に資する、医療情報を取り扱う情報システム・サービスの提供のための適正な運用のため、種々ご検討とご留意のほど、よろしくお願いいたします。	参考意見として承りました。		
15	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	0	用語集	対象事業者の定義：医療機関等から医療情報の加工や保存等の処理に関連する医療情報システムを用いるサービスの提供を受託する事業者のこと。	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「医療機関等から医療情報の加工や保存等の処理に関連する医療情報システム提供を受託する事業者のこと。」	「医療機関等から医療情報の加工や保存等の処理に関連する医療情報システム等提供を受託する事業者のこと。」
16	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	0	全般	本ガイドラインの対象となる事業者について、電子カルテ等の医療情報システムを開発する業者、パッケージ製品を販売する事業者については対象外ということで認識しております。本ガイドラインの対象となるのは、医療情報システムを用いてサービスを提供する事業者(たとえば、電子カルテの外部保存を受託している事業者など)であるとの理解です。 上記認識に基づき、以下1-1,1-2,1-3の意見を提出いたします。	FAQにより整理しましたので、ご参照ください。		
17	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	0	表紙	ガイドラインタイトルを下記に修正してはいかがでしょうか 医療情報を取り扱う情報システムを用いたサービスの提供事業者における安全管理ガイドライン	タイトルの「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」は医療情報を取り扱う情報システム及び/又は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意味であり、こちらは医療情報を受託する情報処理事業者の安全管理ガイドライン改定検討会で議論されたものですので、原案のままとさせていただきます。		
18	欧州ビジネス協会(EBC)医療機器・IVD委員会診療報酬部会	団体	02GL	0	全般	医療情報を取り扱う対象事業者については、第三者認証としてプライバシーマーク認定またはISMS認証を取得することとしているところ、医療情報を直接取り扱わない対象事業者については、プライバシーマーク認定を強く求めるとする一方で、ISMS認証の取得は望ましいとするにとどめている。医療情報を直接取り扱わない事業者についても情報セキュリティに係る公的な第三者認証の取得を求めるのは、「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」に関するQ&A(事例集)A3-6における「医療・介護関係事業者の施設内には様々な個人情報があります。このため、通常は個人データを直接取り扱わない業務であっても、個人情報に接する可能性に配慮する必要があると考えます」という観点からと考えられるが、この状況は個人情報を取り扱うという点においては、医療情報を直接取り扱う事業者と同様であること。 またISMS認証はISO27001(JISQ27001)に基づいた基準に適合した事業者に与えられているが、プライバシーマーク認定はJISQ15001に基づいた基準に適合した事業者に付与されるものの、対応するISO規格が存在せず、今後国際整合を進める上での障壁となりかねないこと。 以上により、『医療情報を直接取り扱わない事業者の場合においても、プライバシーマーク認定またはISMS認証の取得が望ましい。』と同列併記に修正願います。	ご指摘を踏まえて修正いたします。	「医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定の取得を強く求めるほか、ISMS認証の取得も望ましい。」	「医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定またはISMS認証の取得が強く求められる。」
19	個人	個人	02GL	0	全般	組織の情報セキュリティの教育が不十分である問題 情報事故等が発生しても、対応方法をそもそも理解していないので、規程を知らず、規程をまるで無視した杜撰な方法で対応する場合もございます。迅速に適正な対応ができない場合もございます。	参考意見として承りました。		
20	個人	個人	02GL	0	全般	ISMS認証機関、PMS認証機関と共謀し、もみ消すおそれがある問題 ISMS認証機関、PMS認証機関も、他の企業と同様に、営利目的であり、売上を得る必要があるため、利益が優先され、あえて杜撰な審査、不正な金銭等の利益供与によるもみ消し等を行うおそれもございます。 以上、公衆衛生の向上に資する、医療情報を取り扱う情報システム・サービスの提供のための適正な運用のため、種々ご検討とご留意のほど、よろしくお願いいたします。	参考意見として承りました。		
21	個人	個人	02GL	0	全般	「医療情報安全管理ガイドライン」はリスク分析としてISO/IEC27000シリーズのISMS(情報セキュリティマネージメント)を前提にしているが、本ガイドラインはプロジェクトマネージメントで利用されるJIS Q 31000を参考にしている。 前者はリスクを資産価値・脅威・脆弱性に分けて評価している。 本ガイドラインではリスクレベル＝影響度×顕在率としている。通常は発生確率を用いるが、なぜ顕在率にしたのか説明が欲しい。また影響度と資産価値、顕在率と脅威・脆弱性の関係を記述すべきである。 何故、ISMS(情報セキュリティマネージメント)を使用せずにJIS Q 31000を持田法が良いかの記述が欲しい。あるいはISMSでもよいとの記述があっても良い。システム単体での評価はISO/IEC 15408の雰囲気に近いとお思います。	近年IPA等で用いられている用語法を踏まえ、「顕在化率」と表記しています。影響度と資産価値の関係について、情報の安全管理上の重要度に応じた分類を参考に、当該リスクが顕在化した場合の医療情報システムへの機密性、完全性、可用性への影響度合いを総合的に判断した上でリスクの影響度を特定するとして関係性を示しています。ISMSにおける脅威と脆弱性を総合的に考慮したものとして顕在化率を捉えており、「5.1.2 リスク分析」にこの考え方について記載しています。本ガイドラインでは、リスクに応じた対策の実施を重視するリスクベースアプローチを採用しており、ISMS認証の取得をもって本ガイドラインが求める安全管理水準を満たすとは考えておりません。そのため、ISMSで示される事項のうち、純粋なリスクマネジメントプロセス部分に焦点を当てている、JIS Q 31000を参照しております。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
22	個人	個人	02GL	0	用語集	「情報流」、「ICTサプライチェーン」、「顕在率」、「リスクベースアプローチ」という用語の解説を加えるべき。（顕在率は顕在化率の方が分かりやすいと思います） さらに、略語集を作成すべきである。 「医療情報安全管理ガイドライン」:「医療情報システムの安全管理に関するガイドライン」 「クラウド事業者ガイドライン」:「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」 「情報処理事業者ガイドライン」:「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」 「医療情報システム」:「医療情報を取り扱う情報システムやサービス」 「対象事業者」:「医療機関等との契約等に基づいて医療情報システムを提供する事業者」 前回の「情報処理事業者ガイドライン」と同様に参考文献を貼付して欲しい。	ご指摘を踏まえ修正いたします。	（追記）	情報流 「医療情報システムの提供に関わる情報の流れ。」 ICTサプライチェーン 「情報通信技術(ICT)に関わるシステム・サービス等の企画・設計・製造・流通・運用等の各プロセス。または当該プロセスを構成するシステム・組織等のこと。」 顕在化率 「リスクが顕在化する可能性。」 リスクベースアプローチ 「一律の要求事項を定めるのではなく、顕在化しうるリスクの内容に応じた対応方法の選択を実施する手法のこと。」
23	一般社団法人日本医療情報学会事務局	団体	02GL	0	全般	技術が急速に変化することを踏まえて、セキュリティ確保のための技術を一律に定めるのではなく、技術の選択を事業者に預け、説明責任を果たす責務を企業に負わせる今回のガイドラインの改定は、時流を掴んだ、きわめてよい動きであると考えます。今後改定が予定されている医療機関向けの厚生労働省ガイドラインにおいても、詳細な要求要件を謳うことなく、自己アセスメントの実施と、その力のある専門家（HealthcareCIO）の配置の義務づけなど、本改定と同様の方針で本質的な改定が行われることを強く期待します。	賛同意見として承りました。		
24	一般社団法人日本医療情報学会事務局	団体	02GL	0	全般	「情報流」、「顕在（化）率」、「リスクベースアプローチ」という用語の解説を加えるべき。	ご指摘を踏まえ修正いたします。	（追記）	情報流 「医療情報システムの提供に関わる情報の流れ。」 顕在化率 「リスクが顕在化する可能性。」 リスクベースアプローチ 「一律の要求事項を定めるのではなく、顕在化しうるリスクの内容に応じた対応方法の選択を実施する手法のこと。」
25	一般財団法人　信貴山病院	団体	02GL	0	全般	医療情報取り扱いのユーザ（病院）とサービス提供業者間で、下記問題があります。 問題１）Microsoft社のサポート期限の切れたOSで、医療情報を取り扱っている。 問題２）Microsoft社の既知のセキュリティ脆弱性に対するセキュリティ更新プログラムを適用していないOSで医療情報を取り扱っている。 ―――― 状況 ―――― ・２０１８年１０月　亀田医療情報社製電子カルテ「プシュケ」を導入した。 ・電子カルテシステムのシステム連携する他業務システムがある。 ※富士メディカル社：PACS、ソフトマックス社：医事会計システムPlusUS、ユヤマ社 ：調剤システム、京セラ丸善社：栄養管理システムMEDICDIET、日本臨床社：外注検査 システム、フクダ電子社：心電図、・・など ※LAN,ネットワーク分離基盤は、きんでんスピネット、ユニアデックス社で構築した 。 導入時、電子カルテシステムを中心にした業務システムのセキュリティ管理上、事故を予防するために、上記問題１、２を排除した運用企画をした。 その時に、ほどんどの業務システム業者は、「OSをバージョンアップするなんて、したことがない。バージョンアップしても業務システムは、動作すると思うけど、メーカーとして保証しません。検証は、ユーザ側でお願いします」 という回答でした。ご存じのように、奈良県宇陀市立病院におけるランサムウェアによる電子カルテシステムデータ凍結事故事例があります。 このように病院の信頼と、患者の命と、社会的・犯罪性のある事柄に対する責任問題が、医療情報を取り扱う基盤のセキュリティの問題なのです。 現在、日本全国にあるほとんどの病院関係のインフラのセキュリティは、上記業者の回答にあるように、ほどんど、サポート期限の切れたOSで医療情報をあつかっています。富士メディカルなど、日本のトップPACSベンダにおいても、１００％そうでした。 アップデートしないのです。してきてないのが事実のようです。 そして、その責任は、病院のシステム部門が負うのが現状です。あまりにも、システム提供業者は無責任だと思います。	参考意見として承りました。		
26	一般財団法人　信貴山病院	団体	02GL	0	全般	アップデート後の動作保証をメーカとしてしないのならば、アップデートしないことによるリスクをガイドラインに従って、きちんと病院側に説明しろ！と思います。アップデート後の動作保証をメーカとしてしないのならば、どうできるのか・・ 病院側と状況を共有し、再合意形成を維持して、サポートしろ！と思います。 そのようなリスクマネジメントの条項をガイドラインに明記していただきたく。業者の無責任さは、異常です。それを指摘して、問題視してこなかった病院側も異常です。 例：システム運用上、致命的な事故に至る可能性がある事項（例：OSサポート切れ）については、業務システム業者が、顕在化し、ユーザへ説明し、状況を共有したうえで、危機的状況をまねかないことで再合意形成して、それをサービス終了まで、維持することとする。無視や黙秘はダメで、その顕在化とユーザとの合意形成は必須とする。・・など。	本ガイドラインに従って、対象事業者と医療機関等間でのリスクコミュニケーションが適切になされることが重要と認識します。		
27	一般財団法人　信貴山病院	団体	02GL	0	全般	厚労省のガイドライン（医療情報ユーザー側）にも、上記のようなリスクマネジメント事項を盛り込むことが必要だと思います。三省４ガイドラインのすべての統合も視野にいれて、安全なシステム運用、ユーザの危機意識の啓蒙、医療機関のIT基盤構築・サービス提供業者の無責任さ排除のために、ひいては、病院というカテゴリにおける閉鎖的なITリスク放置状態を打破するために、リスクマネジメントにかかるガイドラインの改定、進化を求めます。	参考意見として承りました。		
28	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	（現状） 平成11年4月の通知「診療録等の電子媒体による保存について**1**」 （変更案） 平成11年4月の通知「診療録等の電子媒体による保存について」**1**	ご指摘を踏まえて修正いたします。	「平成11年4月の通知「診療録等の電子媒体による保存について1」」	「平成11年4月の通知「診療録等の電子媒体による保存について」1」
29	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	（現状） 平成14年3月の通知「診療録等の保存を行う場所について2（以下、「外部保存通知」という。） （変更案） 平成14年3月の通知「診療録等の保存を行う場所について」2（以下、「外部保存通知」という。）	ご指摘を踏まえて修正いたします。	「平成14年3月の通知「診療録等の保存を行う場所について2（以下、「外部保存通知」という。）」	「平成14年3月の通知「診療録等の保存を行う場所について」2（以下、「外部保存通知」という。）」
30	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	（現状）医薬**食品**局長 （変更案）医薬**・生活衛生**局長 さらに、保険局長の後に"**、厚生労働省政策統括官(社会保障担当)**"追加	文書発出時はこの通りとなっており、原案のとおりとさせていただきます。		
31	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	（現状） 「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン3」及び「診療録等の外部保存に関するガイドライン4」 （変更案） 「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」**3**及び「診療録等の外部保存に関するガイドライン」**4**	ご指摘を踏まえて修正いたします。	「「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン3」及び「診療録等の外部保存に関するガイドライン4」」	「「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」3及び「診療録等の外部保存に関するガイドライン」4」
32	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	（現状） 「医療・介護関係事業者における個人情報の適切な取扱のためのガイドライン」 （変更案） 「医療・介護関係事業者における個人情報の適切な取扱**い**のためのガイドライン」	ご指摘を踏まえて修正いたします。	「医療・介護関係事業者における個人情報の適切な取扱のためのガイドライン」	「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ドライン」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
33	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	JISQ27000シリーズで用語の定義をしているのは、27002ではなくて、27000 (現状)JISQ27002 (変更案)JISQ27000	ご指摘を踏まえて修正いたします。	「JIS Q 27002」	「JIS Q 27000」
34	一般社団法人 日本画像医療システム工業会	団体	02GL	1	1.1.1	用語の定義のため、参照しているJISと細かい表現まで合わせたほうがいい。 (現状) 機密性(Confidentiality):認可されていない個人、エンティティ又はプロセスに対して、情報を**使用不可又は非公開にする**特性 完全性(Integrity):**資産の**正確さ**および**完全さ**を保護する**特性 可用性(Availability):認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性 (変更案) 機密性(Confidentiality):認可されていない個人、エンティティ又はプロセスに対して、情報を使用**させず、また、開示しない**特性 完全性(Integrity):正確さ**及び**完全**さ**の特性 可用性(Availability):認可されたエンティティが要求したときに、アクセス**及び**使用が可能である特性	ご指摘を踏まえて修正いたします。	機密性(Confidentiality):認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性 完全性(Integrity):資産の正確さおよび完全さを保護する特性 可用性(Availability):認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性	機密性(Confidentiality):認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性 完全性(Integrity):正確さ及び完全さの特性 可用性(Availability):認可されたエンティティが要求したときに、アクセス及び使用が可能である特性
35	一般社団法人 日本画像医療システム工業会	団体	02GL	2	1.1.3	医療情報を取り扱う情報システムやサービス(以下、「医療情報システム」という)と記載しているが、サービスも含めて"医療情報システム"としてしまうと、"サービス"を含まない"システム"の記載がわかりにくくなると思われる。 「医療情報システム等」にして、全文で医療システムのままのものと、等がつくものを見直すべきではないか。	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「医療情報を取り扱う情報システムやサービス(以下、「医療情報システム」という)」	「医療情報を取り扱う情報システムやサービス(以下、「医療情報システム等」という)」
36	一般社団法人 日本画像医療システム工業会	団体	02GL	2	1.1.2	ここは、"並びに"ではなくて"及び"にすべき。 (参考　JISZ8301:2019等)	ご指摘を踏まえて修正いたします。	「平成17年4月における、e-文書法の施行、並びに、個人情報保護法の全面施行に対して」	「平成17年4月における、e-文書法の施行、及び、個人情報保護法の全面施行に対して」
37	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	2,6	P2、1.1.3 P6、2.1	"医療情報システム"や"サービス"をまとめて"医療情報システム"と言い換えるのは適切ではないと考えます。文脈を把握したうえで修文してはいかがでしょうか。 対応案を2つ提示します。 ・対応案1 言い換えを止めて、本文中でも"医療情報システムを用いたサービス"等と記載する。 参考:ISO/IECTS25011:20173.3.2informationtechnologyservice 項番101以降に、関係する例示を記載します。(他多数修正箇所あり) ・対応案2 対象外となる事業者を左記本文に続けて明示してはいかがでしょうか。 修文案: P6、本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システムを用いてサービスを提供する事業者(以下、「対象事業者」という)である。また、本ガイドラインの対象とならない事業者は、患者等から直接医療情報を受領する事業者、及び医療情報を取り扱わず電子カルテ等の単体でのパッケージ製品や機器を開発し販売のみを行う事業者等である。ただし、・・・	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「医療情報を取り扱う情報システムやサービス(以下、「医療情報システム」という)」	「医療情報を取り扱う情報システムやサービス(以下、「医療情報システム等」という)」
38	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	2	1.1.3	・対応案 既存のガイドラインの対象を誤解がないように記載する。 修文案:総務省では、医療情報を電子的に保存するサービスを提供するクラウド事業者に対して、経済産業省は、医療情報を電子媒体経由又はネットワーク経由で受託管理するサービスを提供する情報処理事業者に対してのガイドラインをそれぞれ策定した。	「具体的には」以下で、それぞれの既存のガイドラインの経緯を述べており、原案のとおりとさせていただいます。		
39	一般社団法人 日本画像医療システム工業会	団体	02GL	3	1.1.3	ここは、"並びに"ではなくて"及び"にすべき。 (参考　JISZ8301:2019等)	ご指摘を踏まえて修正いたします。	「総務省が策定したクラウド事業者ガイドライン並びに経済産業省が策定した情報処理事業者ガイドラインからなる」	「総務省が策定したクラウド事業者ガイドライン及び経済産業省が策定した情報処理事業者ガイドラインからなる」
40	一般社団法人 日本画像医療システム工業会	団体	02GL	3	1.1.4	ガイドライン名称を「」でかこむ。記載されているガイドラインは、初版平成26年4月発行。改定した第2版が記載されている平成30年7月発行。 (現状) 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(平成30年7月 総務省)等の情報セキュリティに関するガイドラインが整備され、 (変更案) **総務省**「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**」(平成26年4月、第2版**平成30年7月)等の情報セキュリティに関するガイドラインが整備され、	ご指摘を踏まえて修正いたします。	「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(平成30年7月 総務省)等の情報セキュリティに関するガイドラインが整備され」	「総務省「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」(平成26年4月、第2版平成30年7月)等の情報セキュリティに関するガイドラインが整備され」
41	一般社団法人 日本画像医療システム工業会	団体	02GL	3	1.2	(変更前) クラウド事業者ガイドラインと情報処理事業者ガイドラインが (変更案) クラウド事業者ガイドラインと情報処理事業者ガイドライン**と**が	ご指摘を踏まえて修正いたします。	「クラウド事業者ガイドラインと情報処理事業者ガイドラインが」	「クラウド事業者ガイドラインと情報処理事業者ガイドラインとが」
42	一般社団法人 日本画像医療システム工業会	団体	02GL	3	1.1.4	1.2に"ガイドラインを理解しやすくすることにより"と記載されているように、ガイドラインへの対応が負担なのではなく、ガイドラインの読み込み並びに理解が負担であるからと考えられる。下記のように修正すべきではないか。 修文案:双方のガイドラインの意味を読み取り、理解した上で、どのように対応すべきかを判断するという過程が大きな負担となってきている。	単なる読み込みや理解の負担にとどまらず、それぞれのガイドラインへの対応自体を負担と捉えており、原案のとおりとさせていただきます。		
43	一般社団法人日本医療情報学会事務局	団体	02GL	3	1.1.4	「一律に定めた要求事項の全てに対応することは困難になってきている。」を「一律に定めた要求事項に対応するだけで、情報セキュリティを確保することは困難になってきている。むしろ、一律に要求事項を定めることは、情報セキュリティの低下をもたらす可能性の方が高い。」と変更。	一律に要求事項を定めることが、情報セキュリティの低下をもたらす可能性が高いとまでは言えず、原案のとおりとさせていただきます。		
44	HEASNET事務局	団体	02GL	4	1.2	リスクコミュニケーションの用語の意図が、医療機関等と事業者で異なってしまう可能性があるため、p.30の注釈22に示している事項を、用語集に定義をきちんと明記してはどうか。	ご指摘を踏まえて、用例集に追加いたします。	(追記)	リスクコミュニケーション 「リスクマネジメントの実効性を高めるために、医療機関等と対象事業者の双方によって実施される活動のこと。対象事業者から医療機関等への情報提供等の一方向的な活動だけでなく、医療機関等の疑問や要求に応えながら、共通理解を得る双方向的な活動が重要視される。」
45	一般社団法人 日本画像医療システム工業会	団体	02GL	4	1.2	箇条書きがあるが、それぞれ文章になっているので、最後に句点("。")を追加。 句点をおかない場合は、体言で止める。	ご指摘を踏まえて修正いたします。	□他の規格・ガイドラインとの整合性の確保に留意しながら、過去のガイドラインの遵守と同等の安全管理水準が確保されるようにする □医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する □セキュリティ対策の妥当性と限界について正しい共通理解と明示的な合意のもと医療情報システムを運用するために、リスクコミュニケーションを重視する □医療情報システムに関連する法令の求めに対して対策の抜け漏れを防止するために、医療情報の取扱いにおいて留意すべき点や制度上の要求事項を明らかにする	□他の規格・ガイドラインとの整合性の確保に留意しながら、過去のガイドラインの遵守と同等の安全管理水準が確保されるようにする。 □医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する。 □セキュリティ対策の妥当性と限界について正しい共通理解と明示的な合意のもと医療情報システムを運用するために、リスクコミュニケーションを重視する。 □医療情報システムに関連する法令の求めに対して対策の抜け漏れを防止するために、医療情報の取扱いにおいて留意すべき点や制度上の要求事項を明らかにする。

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
46	一般社団法人 日本画像医療システム工業会	団体	02GL	4	1.2	リスクコミュニケーションの用語の意図が、医療機関等と事業者で異なってしまう可能性があるため、p.30の注釈22に示している事項を、用語集に定義をきちんと明記してはどうか。	ご指摘を踏まえて修正いたします。	（追記）	リスクコミュニケーション 「リスクマネジメントの実効性を高めるために、医療機関等と対象事業者の双方によって実施される活動のこと。対象事業者から医療機関等への情報提供等の一方向的な活動だけでなく、医療機関等の疑問や要求に応えながら、共通理解を得る双方向的な活動が重要視される。」
47	グーグル・クラウド・ジャパン合同会社	団体	02GL	4	1.2	本記の記述については、特定の技術要件を明示しそれを要求しているように受け取れましたが、実際のところは如何でございますでしょうか。	本ガイドラインは、「医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する」という方針に基づき、可能な限り一律の要求事項を排すよう努めていますが、医療情報システム特有の考慮事項として必要と考えられる個別の要求事項については、これを記述しているものです		
48	アマゾン ウェブ サービス ジャパン株式会社	団体	02GL	4	1.2 脚注7	同脚注には、「JIS Q 31000:2019やJIS Q 27001:2014等」とJISQのみの記載がありますが、20ページの脚注15の記載と同様に、対応するISO/IECも併記するのが良いと考えます。	ご指摘を踏まえて修正いたします。	「JIS Q 31000:2019やJIS Q 27001:2014等」	「JIS Q 31000:2019(ISO 31000:2018)やJIS Q 27001:2014 (ISO/IEC 27001:2013)等」
49	個人	個人	02GL	4	1.2	「一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する」を「一律に定めた要求事項に対応するベースラインアプローチだけでは情報セキュリティを確保することは困難になってきているので、リスクベースアプローチに基づいた詳細リスク分析との組合せアプローチによるリスクマネジメントプロセスを定義する。」に修正する。(参考資料：医療機関等向けISMS ユーザーズガイド－ ISMS 認証基準（Ver.2.0）P51 2004 年11 月8 日財団法人日本情報処理開発協会）	当該記述は端的に策定方針を述べたものであり、原案のとおりとさせていただきます。		
50	個人	個人	02GL	4	1.2	１番目の黒ぽちのあとに2番目の黒ぽちとして以下を加える。 「「クラウド事業者ガイドライン」は「クラウドサービス事業者」、 「情報処理事業者ガイドライン」は「医療情報を受託管理する情報処理事業者」を対象としていた。本ガイドラインが対象とする事業者は、それを含めた形で事業者の範囲を広め、医療機関等との契約等に基づいて医療情報システムを提供する事業者を対象とした。また、医療機関等に提供する医療情報システムに必要な資源や役務を提供する事業者や、患者等の指示に基づいて医療機関等から医療情報を受領する事業者も対象とした。 「クラウド事業者ガイドライン」にあった、オンライン診療とPHRに関すする記述は本ガイドラインでも記述して欲しい。	本ガイドラインはこれまでの両省ガイドラインの対象を広げるものではなく、原案のとおりとさせていただきます。		
51	一般社団法人日本医療情報学会事務局	団体	02GL	4	1.2	「整理・統合する。」を「整理・統合し、クラウド事業者ガイドラインと情報処理事業者ガイドラインを廃止する。」と変更。	趣旨は同様のため、原案のとおりとさせていただきます。		
52	キヤノンメディカルシステムズ株式会社	団体	02GL	5,44	1.3	別紙2の旧ガイドラインとの対比表の利用方法をもう少し解説した方がよいと思います。一読して別紙2の位置付けが理解できないと思われます。	ガイドライン記載のとおり、別紙2については、従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を医療情報安全管理ガイドライン（第5版）との対応関係を踏まえ対策項目として整理・統合したものであり、医療機関等が医療情報安全管理ガイドラインを遵守できるような対策設計のための対策項目の確認という位置づけとしてご活用ください。		
53	HEASNET事務局	団体	02GL	6	2.1	介護事業者も医療情報を取り扱うことがある旨を、もっと分かりやすく示してはどうか。	介護事業者については、図2-1で医療機関等の一部であることを明記しているほか、用語集の医療機関等で記述しております。		
54	一般社団法人 日本画像医療システム工業会	団体	02GL	6	－	現2省のGLからの流れで言えば当然ですが、P6の「医療情報システムを提供する事業者」には、PACSやRIS等のシステム製品販売事業者は対象外であることの明記が欲しい。 契約に従った「納入」を持って売買契約完了し、その後は購入した利用者での管理・運用責任です。 P6 図3-4の説明等では、運用中も対象事業者が合意を維持して運用するように記載されている。つまり、売り切りのようなシステム、製品に関しては、本ガイドラインの対象外であることを明確にしておく必要があると考える。	FAQにより整理しましたので、ご参照ください。		
55	一般社団法人 日本画像医療システム工業会	団体	02GL	6	2.1	介護事業者も医療情報を取り扱うことがある旨を、もっと分かりやすく示してはどうか。	介護事業者については、図2-1で医療機関等の一部であることを明記しているほか、用語集の医療機関等で記述しております。		
56	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	6	図2-1	医療機関等との契約等に基づいて医療情報システムを用いるサービスを提供する事業者	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	図2-1 	図2-1 
57	アマゾン ウェブ サービス ジャパン株式会社	団体	02GL	6, 11	1及び3	AWSとしましては、第一に「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事業者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。 第二に、6ページの「ただし、医療機関等と直接的な契約関係になくても、医療機関等に提供する医療情報システムに必要な資源や役務を提供する事業者や、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は本ガイドラインにおける対象事業者となる」との記述について、責任共有モデルの考え方にもとづきサービス提供するクラウド事業者は対象事業者にはあたらない場合があることを明記すべきと考えます。 第三に、10ページの第三パラグラフについて、「対象事業者Bは対象事業者Aに、AB間の契約にもとづき、対象事業者Cは対象事業者Bに対して、BC間の契約にもとづき、対象事業者Aが医療機関等に対してリスクマネジメントの実施状況と制度上の要求事項への対応状況を報告することを支援すること。」とし、各当事者が、仮に対象事業者に該当するとしても、当事者間の契約に基づき、サプライチェーンにおいて置かれた立場を反映した相応の責任を果たすものであることを明記してはどうか、と考えます。	FAQにより整理しましたので、ご参照ください。		
58	一般社団法人 日本画像医療システム工業会	団体	02GL	7	2.2	P7, 2.2代表的な提供形態が記載されているが、図3-4での開発フェーズと運用フェーズとで事業者が異なる場合を想定した記載等も必要になる。つまり、図3－4で開発フェーズの合意と運用フェーズの合意とが独立する場合もありえる。これを明記する必要があると考える。	FAQにより整理しましたので、ご参照ください。		
59	キヤノンメディカルシステムズ株式会社	団体	02GL	7	2.2	代表的な提供形態として下記の事例も説明が必要と思われます。 1）地域連携ネットワーク運営主体（総務省ガイドライン第1版で説明） 2）販売会社（医療機関と各種事業者との間に入るケース）	本ガイドラインでは、提供形態を網羅することは困難なことから、医療情報システムの構成要素をアプリケーション、プラットフォーム、インフラの3種類に分類した上で、各々の構成要素を1又は複数の事業者で提供するケースに応じて、対象事業者に求められる対応について記載いたしました。 また、販売会社については、FAQにより整理しましたので、ご参照ください。		
60	キヤノンメディカルシステムズ株式会社	団体	02GL	7,9	2.2 図2-2	P46用語集では下記と解釈できるが、図中での使われ方と合っていません。むしろ、SaaS、PaaS及びIaaSに言葉は使わない方が良いと思われます。 IaaS＝インフラ PaaS＝インフラ＋ミドルウェア＋OS SaaS＝インフラ＋ミドルウェア＋OS＋アプリケーション 例えば、図2-5ですと、対象業者BがPaaSでインフラ＋ミドルウェア＋OSを提供し、対象業者 CがIaaSでインフラを提供します。インフラが重複しており、どのような運用になるのかがイメージできません。	FAQにより整理しましたので、ご参照ください。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
61	キヤノンメディカルシステムズ株式会社	団体	02GL	7	2.2	アプリケーション、プラットフォーム及びインフラが具体的にどのような要素なのかを説明する必要があります。 図2-2で使われているSaaS、PaaS、IaaSと同意義になっており、違和感があります。	用語集及びガイドライン内の図表上でのSaaS、PaaS及びIaaSの取扱いについて齟齬は見られず、原案のとおりとさせていただきます。		
62	グーグル・クラウド・ジャパン合同会社	団体	02GL	7−10,33−37	全般	図2-2～2-6においては、構成要素をアプリケーション（SaaS）、プラットフォーム（PaaS）、インフラ（IaaS）で定義しているように見える一方で、P.32−37の「5.2リスクアセスメント及びリスク対応の実施例」部分における図例に関しては、オンプレミス（サーバ・クライアントモデル）を意識されているように見受けられます。医療情報システム・サービスにおきましても、昨今議論されている「クラウド・バイ・ディフォルト」を意識されているという理解で問題ございませんでしょうか。	本ガイドラインは、クラウド・バイ・デフォルトを念頭に置いたものではありません。		
63	株式会社セールスフォース・ドットコム	団体	02GL	8	2.2.2	事業者Aが事業者Bを調達したケースでも、契約上は、事業者Bが医療機関と直接契約される場合があることを含んでもいただきたい。	FAQにより整理しましたので、ご参照ください。		
64	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	8	2.2.1	対象事業者Aが1社で医療情報システムを用いるサービスを提供するケース（図 2-3）。	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「対象事業者Aが1社で医療情報システムを提供するケース（図 2-3）」	「対象事業者Aが1社で医療情報システム等を提供するケース（図 2-3）」
65	一般社団法人 日本画像医療システム工業会	団体	02GL	10	2.2.3	B事業者がA事業者に無断で医療機関との契約内容を変更した場合には、A事業者には責任を持てない。従って、B事業者からA事業者への直接的通知、あるいは利用者を介した間接的通知の責務を謳うべきでは、と考える。	FAQにより整理しましたので、ご参照ください。		
66	グーグル・クラウド・ジャパン合同会社	団体	02GL	10	2.2.3	ここでは、マルチクラウド若しくは、マルチベンダーを想定されているかと思いますが、この場合、対象事業者Aが特段サービスの依存・契約関係に無い対象事業者Bの構成要素を含めることは、困難であると思われます。	FAQにより整理しましたので、ご参照ください。		
67	株式会社セールスフォース・ドットコム	団体	02GL	10	2.2.3	文言「本ガイドラインが求める対応の対象範囲に、対象事業者Bが提供する構成要素を含めること。」を削除いただきたい。	FAQにより整理しましたので、ご参照ください。		
68	富士通株式会社	団体	02GL	10	2.2.3	「個人情報保護法」では、医療情報システムの管理者に「安全管理・確保義務」がある、と規定されている。 これを受けて、厚労省のガイドラインでは、医療情報の取り扱いに関し、責任所在は医療機関側にある、とされている。 また、複数事業者にて医療情報システムが構成されている場合、事業者Aが他事業者も構成要素として含めることは、事業者間の契約事項がないため、現実的ではない。 このことから、異なる事業者間でのとりまとめは、契約者である医療機関側が実施することである。	FAQにより整理しましたので、ご参照ください。		
69	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	10	2.2.3	対象事業者A、対象事業者Bはそれぞれ独立して自社の医療情報システムについて本ガイドラインに基づくリスクマネジメント及び制度上の要求事項への対応を行い、医療機関等へ医療情報システムを用いるサービスを提供すること。	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「医療情報を取り扱う情報システムやサービス（以下、「医療情報システム」という）」	「医療情報を取り扱う情報システムやサービス（以下、「医療情報システム等」という）」
70	一般社団法人 日本画像医療システム工業会	団体	02GL	11	3	3のタイトルと3.1とのタイトルとの間の文章を、ぶらさがり段落と呼び、JIS(日本産業規格)等では禁止している構成である。 本ガイドラインは、JISではないが、特に問題ないことはJISの書式、ルールに従うのがいいのではないかと思われます。	行政文書では通例として見られる構成であり、原案のとおりとさせていただきます。		
71	一般社団法人 日本画像医療システム工業会	団体	02GL	11	3.1.1(1)	解釈されていることの根拠例を、脚注に参考として示してほしい。	医療機関等においても、患者に対し私法上の守秘義務を負っていると解されるところ、その旨を記述したものです。		
72	富士通株式会社	団体	02GL	11	3	医療機関等がセキュリティについての専門性に乏しいことを前提することは、セキュリティ事案の事例から見ても、逆行しているといえる。 個人情報保護法「安全管理・確保義務」の規定により、個人情報の安全管理における責任所在は、医療機関であることを前提にしなくてはならない。	本ガイドラインにおいても、医療機関等が管理する個人情報の安全管理義務は、医療機関にあることを前提にしておりますが、対象事業者と医療機関等の間において、セキュリティに関する専門性に一定の差異があることは踏まえるべきと考えます。		
73	一般社団法人 日本画像医療システム工業会	団体	02GL	12	3.1.1(1)	図中の"委託契約"は、本文の要旨、図3-2, 3-3との整合から、"委託契約等"にすべき。	ご指摘を踏まえて修正いたします。	図3-1  図 3-1 善管注意義務と守秘義務について	図3-1  図 3-1 善管注意義務と守秘義務について。
74	アマゾン ウェブ サービス ジャパン株式会社	団体	02GL	12	3.1.1	前記のとおり、個人情報保護法上、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こととなっている場合には、委託を受けたことにはならないため、同じく「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事業者にあたらない場合があること」を明示すべきと考えます。	FAQにより整理しましたので、ご参照ください。		
75	一般社団法人日本医療情報学会事務局	団体	02GL	12	3.1.3 図3－3	医療機関と対象事業者の間の「契約責任・不法行為責任」の間の矢印を一方向の矢印から両方向の矢印へ変更。	図は典型的な例を示したものですので、原案のとおりとさせていただきます。		
76	HEASNET事務局	団体	02GL	13	3.1.3	項の内容に対して、タイトルのニュアンスが異なるのではないか。修正案として"事故等発生時に考えうる義務と責任"ではどうか。	ご指摘を踏まえて修正いたします。	「3.1.3 事後責任」	「3.1.3. 情報セキュリティ事故等発生時における義務と責任」
77	一般社団法人 日本画像医療システム工業会	団体	02GL	13	3.1.3	項の内容に対して、タイトルのニュアンスが異なるのではないか。修正案として"事故等発生時に考えうる義務と責任"ではどうか。	ご指摘を踏まえて修正いたします。	「3.1.3 事後責任」	「3.1.3. 情報セキュリティ事故等発生時における義務と責任」
78	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	13	3.1.2	これに対し、対象事業者は、医療機関等に対し専門的な医療情報システムを用いるサービスを提供する事業者であり、	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「これに対し、対象事業者は、医療機関等に対し専門的な医療情報システムを提供する事業者であり」	「これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり」
79	一般社団法人 日本画像医療システム工業会	団体	02GL	14	3.2	3.2のタイトルと3.2.1とのタイトルとの間の文章を、ぶらさがり段落と呼び、JIS(日本産業規格)等では禁止している構成である。 本ガイドラインは、JISではないが、特に問題ないことはJISの書式、ルールに従うのがいいのではないかと思われます。	行政文書では通例として見られる構成であり、原案のとおりとさせていただきます。		
80	一般社団法人 日本画像医療システム工業会	団体	02GL	15	3.2 図3-4	「合意」が「契約前」であることの明示には大いに賛成する。	賛同意見として承りました。		
81	一般社団法人 日本画像医療システム工業会	団体	02GL	15	3.2 図 3-4	契約終了フェーズにて取り扱いを確定させたうえで、委託契約終了後も残る守秘義務契約はありえるため、合意の維持は契約終了の箱まで伸ばすべきである。	ご指摘を踏まえて修正いたします。	図3-4  図 3-4 医療情報システムのライフサイクル	図3-4  図 3-4 医療情報システム等のライフサイクル。

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
82	(株)神戸デジタル・ラボセキュリティ事業部	団体	02GL	16	3.2.3	・意見内容1 「3.2.3.危機管理対応時の義務及び責任」の中に以下の文言を追加して欲しい。 「対象事業者は、危機管理対応時において危機管理対応に支障が生じない限り、当該医療機関から要求がある場合は、当該医療機関が要求する当該医療機関に関わる事故に関する詳細な情報を提供しなければならない。また、複数医療機関の情報を取り扱っている場合、当該医療機関ログ情報等が開示できるように、医療機関単位に情報が抽出できる仕組みや対処手段をあらかじめ用意しなければならない」	ご意見につきましては、今後の取組の参考とさせていただきます。		
83	一般社団法人 日本画像医療システム工業会	団体	02GL	16	3.2.2	P16 3.2.2 に、すべてに開発フェーズが有る事が前提のような記載になっている。個別案件での開発が想定されていない提供サービスもある。	開発フェーズについては、ご指摘の個別案件での開発のみならず、機器・端末のアップデートや機能更新に伴う開発（保守開発）や、各医療機関等での初期設定といった、運用フェーズの前段階を広く含む概念として捉えております。その旨を明確にするため、本文に追記いたしました。	「「開発フェーズ」には新規の開発（新規開発）だけでなく、機器・端末のアップデートや機能更新に伴う開発（保守開発）も含むものとする。」	「「開発フェーズ」には新規の開発（新規開発）だけでなく、機器・端末のアップデートや機能更新に伴う開発（保守開発）や各医療機関等での初期設定といった、運用フェーズの前段階も広く含むものとする。」
84	一般社団法人 日本画像医療システム工業会	団体	02GL	16	3.2.3	P.16 3.2.3などで使われている「情報事故」は、「情報**セキュリティ**事故」が適切な表現だと思います。	ご指摘を踏まえて修正いたします。	「情報事故」	「情報セキュリティ事故」
85	一般社団法人 日本画像医療システム工業会	団体	02GL	16	3.2.2	運用と平行に開発が行われることは一般的にあり得るため、それを明記すべきである。 修文案:「移行することも考えられる。」→「移行することや、運用中に開発フェーズが並行発生することも考えられる。」	ご指摘を踏まえて修正いたします。	「したがって、開発フェーズは1度のみ発生するとは限らず、運用フェーズから再度開発フェーズに移行することも考えられる。」	「したがって、開発フェーズは1度のみ発生するとは限らず、運用フェーズから再度開発フェーズに移行することや、運用中に開発フェーズが並行発生することも考えられる。」
86	HEASNET事務局	団体	02GL	17	3.2.3	安全管理GLにて厚生労働省への報告が求められている事項を記載してはどうか。	ご指摘を踏まえて注釈に追記いたします。	（追記）	「医療情報安全管理ガイドラインでは、情報セキュリティ事故発生時に厚生労働省への連絡を実施することが求められている。」
87	一般社団法人 日本画像医療システム工業会	団体	02GL	17	3.2.3	安全管理GLにて厚生労働省への報告が求められている事項を記載してはどうか。	ご指摘を踏まえて注釈に追記いたします。	「また、対象事業者は、発生した情報セキュリティ事故について、速やかに善後策を講じなければならない」	（挿入） 「医療情報安全管理ガイドラインでは、情報セキュリティ事故発生時に厚生労働省への連絡を実施することが求められている。」
88	一般社団法人 日本画像医療システム工業会	団体	02GL	17	3.2.3	なぜここだけ「べき」としているのか？行政機関への説明に必要となっても提供しなくても良いように読めるため、下記のように修正してはどうか。 修正案:できる限り詳細な情報を提供すること	発生した情報事故に関し、個々の患者、行政機関や社会へ説明・公表を行う責務を有しているのは、一義的には医療機関等であり、事業者においても、そのサポートとしてできる限り詳細な情報を提供することが望まれますが、医療機関等と事業者間の契約を超えて法的な拘束力を伴うものではないと考えられるところ、原案のとおりとさせていただきます。		
89	一般社団法人 日本画像医療システム工業会	団体	02GL	18	－	「セキュリティ開示書」はJAHISだけでなくJIRAも共同制作者であるので、「JIRAのJESRA TR 0039 *B」も記載すべき。	ご指摘を踏まえて修正いたします。	「保健医療福祉情報システム工業会（JAHIS）が策定する」	「一般社団法人日本画像医療システム工業会(JIRA)および一般社団法人保健医療福祉情報システム工業会（JAHIS）による」
90	一般社団法人 日本画像医療システム工業会	団体	02GL	18	4.1 脚注13	サービス仕様適合開示書の説明では、対象事業者が、自ら提供するサービスの仕様につき、本ガイドラインへの適合状況を医療機関等へ開示するために作成するための資料のこと。と記されている。事業者にとっては、本書のみを参考にすればいいので効率的かもしれない。しかし、医療機関等にとっては、本ガイドラインは参考にしない。 医療機関等にとっては、自組織が、“医療情報安全管理ガイドライン”を実施するために提供事業者の開示された情報で何がたりて、何が不足しているか容易にわかることが望まれる。さらに、医療機関等が提供事業者を選択するにあたり、簡単に複数のものを比較できるような書式等が望まれるのではないかと思われる。 **従って、P18の脚注にある参照チェックリストの記載は、本文に記載すべき。**	参考情報として注釈に記載をしており、原案のとおりとさせていただきます。		
91	一般社団法人 日本画像医療システム工業会	団体	02GL	18	4	4のタイトルと4.1とのタイトルとの間の文章を、ぶらさがり段落と呼び、JIS(日本産業規格)等では禁止している構成である。本ガイドラインは、JISではないが、特に問題ないことはJISの書式、ルールに従うのがいいのではないかと思われます。	行政文書では通例として見られる構成であり、原案のとおりとさせていただきます。		
92	一般社団法人 日本画像医療システム工業会	団体	02GL	18	4.1	“本節では、～表4.1に示す。”は、少し日本語が不自然。“本節では、”は削除すべきではないか。	ご指摘を踏まえて修正いたします。	「本節では、合意形成のために提供すべき情報とは何であるかを表 4.1に示す」	「合意形成のために提供すべき情報とは何であるかを表 4.1に示す」
93	一般社団法人 日本画像医療システム工業会	団体	02GL	18	4.1	医療機関等におけるリスクマネジメントに対するリテラシーのレベルは、各々異なり、例えば、大学病院等の情報管理専門の部門が設置されている医療機関と、専門部門のない診療所では、リテラシーのレベルは大きく異なる。 医療機関等へ「共通理解」を求める場合、個別の医療機関ごとに運用規定の制定等が必要となると想定され、作業量は膨大となり、医療機関等、対象事業者の双方にとって大きな負荷となる。厚生労働省の「医療情報システムの安全管理に関するガイドライン」に照らし、「最低限実施すべき事項」と「推奨される事項」を整理した形で、合意形成するべき内容を定めるべきではないか。	表 4-1に示した合意形成のために提供すべき情報については、厚生労働省の「医療情報システムの安全管理に関するガイドライン」の要求事項も踏まえて、整理したものです。対象事業者から医療機関等に対しては適切に情報提供がなされた上で、合意形成されることが重要と考えます。		
94	(一社)保健医療福祉情報システム工業会[JAHIS]	団体	02GL	18	4.1 脚注13	例えば、保健医療福祉情報システム工業会（JAHIS）が策定する「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」があり、当該チェックリストが対象とする医療情報システムを用いるサービスを提供する対象事業者においては、当該チェックリストを参考とすることが有効である。	「医療情報を取り扱う情報システムやサービス」については「医療情報システム等」と定義し、これを踏まえて記述を修正いたします。	「例えば、保健医療福祉情報システム工業会（JAHIS）が策定する「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」があり、当該チェックリストが対象とする医療情報システムを提供する対象事業者においては、当該チェックリストを参考とすることが有効である。」	「例えば、一般社団法人日本画像医療システム工業会(JIRA)および一般社団法人保健医療福祉情報システム工業会（JAHIS）による「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」があり、当該チェックリストが対象とする医療情報システムを提供する対象事業者においては、当該チェックリストを参考とすることが有効である。」
95	(株)神戸デジタル・ラボセキュリティ事業部	団体	02GL	19	表4―1	・意見内容2 「表4―1医療機関等へ情報提供すべき項目」の最終行に以下の条項を追加して欲しい。 【「目的」列の項目】 「危機管理対応時」に医療機関等との意識共有をするために情報提供すべき項目 （※「意見内容4」にて追加する「危機管理対応時のインシデントレスポンス」の条項を参照） 【「情報提供すべき項目」列の項目】 インシデント対応について医療機関等と事前の準備内容、実施内容（「運用管理規程に含める事項（5.1.6参照）」の中でも構わない） インシデント発生時の初期対応時から事後対応時まで随時発生する報告内容 インシデント発生時の当該医療機関から依頼のあった事故に関する詳細な情報	ご意見につきましては、今後の取組の参考とさせていただきます。		
96	一般社団法人 日本画像医療システム工業会	団体	02GL	19	4.1	右の列の項目が、別紙1に対応している。 (1) 対応がわかるように①~⑮の番号をつけたらどうか。 (2) 表の右の列が先頭の列にしたほうがわかりやすいのではないか。 (3) 表の目的の列に記載されている項目が、”目的“でなく、提供すべき項目の説明になっているものがある。	原案にても特段理解に支障がなく、原案のとおりとさせていただきます。		
97	一般社団法人 日本画像医療システム工業会	団体	02GL	19	4.2	個別の例を出すのではなく、医療機関等が安全管理ガイドラインを遵守する旨を記載してはどうか。 修文案:例えば、医療情報システムが堅牢なアクセス制御機能を持っていたとしても、医療機関側では安全管理ガイドラインを遵守した適切な運用や管理が求められる。	本記述は、後述の「合意形成にあたり、医療機関等における運用管理も踏まえた形で、役割分担を定めること」が必要であることの理解を促すために例示を用いており、原案のとおりとさせていただきます。		
98	グーグル・クラウド・ジャパン合同会社	団体	02GL	19	4	P.28「⑤小型半導体メモリの利用における考慮事項」においても、同メモリの使用を行うことが出来ないように配慮することが望ましい、との記述があることから、当該部分については不要であると考えます。	「運用管理規定に含める事項」における「医療情報を格納する記憶媒体の管理方法」とは、小型半導体メモリの利用に関わらず、個人情報を格納する記憶媒体の管理方法として、保管や取扱いの方法及び保管や取扱いに係る履歴の記録について運用管理規程に含めることを求めるものであり、必要な項目であると考えます。		
99	富士通株式会社	団体	02GL	19	4.1	表4-1医療機関等へ情報提供すべき項目に記載されている、 ・リスクアセスメントの成果物 ・運用管理規定に含める事項に示されるドキュメント は不適切と思われる。 個人情報保護法「安全管理・確保義務」の規定、厚労省ガイドライン4章、6.2章により、医療情報システム全体でのリスクアセスメント、運用規定の制定等は、医療機関が行うものである。	本記述は、医療情報システム全体でのリスクアセスメント、運用規定の制定等は、医療機関が行うものであることは前提として、対象事業者は、その提供する医療情報システムについて、リスクアセスメントの成果物等を医療機関等へ情報提供することを求めているものです。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
100	個人	個人	02GL	19	4.2	責任分界点という用語も使用して欲しい。	本ガイドラインにおいては、責任分界点という用語は用いず、役割分担としております。		
101	HEASNET事務局	団体	02GL	20	4.4	4.1の事項が前提となっている旨、記載してはどうか。	本記述は、プライバシーマーク認定等が、医療情報を取り扱う事業者としての最低限の適格性を医療機関等へ示す公的な第三者認証として位置づけられる一方で、本ガイドラインが求める安全管理水準を直接充足するものではないことを為念的に記述したものであり、原案のとおりとさせていただきます。		
102	一般社団法人 日本画像医療システム工業会	団体	02GL	20	4.4	4.1の事項が前提となっている旨、記載してはどうか。	本記述は、プライバシーマーク認定等が、医療情報を取り扱う事業者としての最低限の適格性を医療機関等へ示す公的な第三者認証として位置づけられる一方で、本ガイドラインが求める安全管理水準を直接充足するものではないことを為念的に記述したものであり、原案のとおりとさせていただきます。		
103	個人	個人	02GL	20, 31	4.4	これまでの様々な経験等から、当ガイドライン（案）の下記の記載につきまして、少なくとも次の問題が憂慮されるよう存じましたので、ご検討のほど、よろしくお願いいたします。（1通目） 「医療情報の機微性に鑑み、対象事業者は、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、情報セキュリティに係る公的な第三者認証として、プライバシーマーク認定またはISMS認証を取得すること。なお、医療情報を直接取り扱わない対象事業者の場合においても、プライバシーマーク認定の取得を強く求めるほか、ISMS認証の取得も望ましい。また、これら以外の公正な第三者の認証等として、セキュリティ管理に係る内部統制保証報告書があり、対象事業者は、プライバシー認定及びISMS認証の取得と併せて当該報告書による保証を受けることも望ましい。ただし、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすわけではないことに留意すること。」（20ページ） 「(カ)事故発生時の対応方法及び医療機関等への報告方法 対象事業者は、事故発生時の対応方法及び医療機関等への報告方法として、情報事故が発生した場合の被害拡大防止のための対応方法や緊急時の代替手段、原因調査のためのログ等の記録の保全及び医療機関等への報告タイミングや報告フローを運用管理規程に含めること。」（31ページ） ○　問題1 委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、委託先、その再委託先等で情報セキュリティ、個人情報の問題を巧妙にもみ消すおそれがあること	本ガイドラインにおいては、プライバシーマーク認定またはISMS 認証の取得について、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の情報セキュリティに係る公的な第三者認証として位置づけており、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすものとは位置づけておりません。		
104	個人	個人	02GL	20, 31	4.4	○　問題2 委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、内部でもみ消していた場合、ISMS認証機関に通報しなければ、情報セキュリティ、個人情報の問題が放置されてしまう場合があること	本ガイドラインにおいては、プライバシーマーク認定またはISMS 認証の取得について、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の情報セキュリティに係る公的な第三者認証として位置づけており、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすものとは位置づけておりません。		
105	個人	個人	02GL	20, 31	4.4	○　問題3 委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、内部でもみ消していた場合、ISMS認証機関が毎年の審査時にも情報セキュリティ、個人情報の情報事故等の問題に何年間も全く気付かない場合があること	本ガイドラインにおいては、プライバシーマーク認定またはISMS 認証の取得について、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の情報セキュリティに係る公的な第三者認証として位置づけており、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすものとは位置づけておりません。		
106	個人	個人	02GL	20, 31	4.4	○　問題4 委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、組織内部の情報セキュリティに関する規程が曖昧である場合（情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント等の曖昧な定義等）、情報セキュリティ、個人情報等の情報事故の問題をもみ消せること 　委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、外部のISMS認証機関は、審査時にも実際より情報セキュリティ、個人情報の問題が過少申告されていることに全く気が付かない場合もあります。ISMSの事務局の情報セキュリティに関するインシデント一覧と運用組織の障害管理台帳等のインシデント一覧との二重帳簿、裏帳簿等で悪く運用されている場合があります。故意に都合よくインシデント件数を操作できる場合があります。	本ガイドラインにおいては、プライバシーマーク認定またはISMS 認証の取得について、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の情報セキュリティに係る公的な第三者認証として位置づけており、これら認証の取得をもって、本ガイドラインが求める安全管理水準を満たすものとは位置づけておりません。		
107	個人	個人	02GL	20, 31	4.4	○　問題5 情報セキュリティに関する不正を告発した通報者が保護されない場合があること 経験上、情報セキュリティの社内規定違反も対象であるとの勤務していたシステム運用委託先のN社の公益通報者保護規定に明記もあり、公益通報者としてシステム運用委託先のN社の通報窓口に通報しておりましたが、システム運用委託先のN社との私の労働者派遣法に基づく派遣契約をシステム運用委託先のN社側から一方的に切るという悪質で重大な問題が発生しました。システム運用委託先のN社は、私が指摘した情報セキュリティに関する問題をもみ消したいがために、システム運用委託先のN社が一方的に私を辞めさせたと考えております。公益通報者保護法、社内の公益通報者保護規程で通報者を適切に保護するべきであると存じます。通報者を適切に保護するようガイドラインに含めていただきたく存じます。	公益通報者保護法等に係る取扱いについては、本ガイドラインの射程外となります。		
108	個人	個人	02GL	20, 31	4.4	委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、組織内部の情報セキュリティに関する規程が曖昧である場合（情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント等の曖昧な定義等）、情報セキュリティ、個人情報等の情報事故の問題をもみ消せること 　補足いたしますと、報告対象の情報セキュリティの問題の定義を曖昧にして、情報事故をもみ消す方法以外にも、システム関連業務の委託先、その再委託先等のISMS認証、PMS認証等の適用範囲に医療機関等がそれらの委託先等との間で委託契約した業務範囲が含まれていないので、杜撰に情報が取り扱われるおそれもございます。つまり、委託先、その再委託先等がISMS認証、PMS認証等を取得しているといっても、ISMS認証、PMS認証等の適用範囲外である場合、ISMS認証、PMS認証等のとおりに適切に情報が取り扱われるかは、不透明であり、情報事故をもみ消せる場合もあると存じます。例えば、個人情報の記載された記録媒体を紛失、漏えい等があっても、その個人情報は、管理対象の情報に含まれていないと言って、もみ消す場合も憂慮されます。契約前に、必ず、委託先、その再委託先等のISMS認証、PMS認証等の適用範囲の開示を受け、適用範囲外の情報セキュリティの問題についての対応について協議し、理解し、対策を講じておく必要があると存じます。ISMS、PMS等の規格としての必須ルールとして、それらの認証取得者の適用範囲の開示を発注者等のステークホルダーへの義務化することも経済産業省としてもぜひご検討ください。	参考意見として承りました。		
109	アマゾン ウェブ サービス ジャパン株式会社	団体	02GL	20	4.4	「プライバシーマークの認定やISMS認証又は他の国際的に認知された認証の取得などによる第三者評価を行うことが望ましい」との記述とすべき。	これまでの両省ガイドラインを引き継ぎ、現時点においては、医療情報を取り扱う事業者としての最低限の適格性を医療機関等へ示す公的な第三者認証として、プライバシーマーク認定及びISMS認証が適当と考えます。		
110	個人	個人	02GL	20, 31	4.4	委託先、その再委託先等は、情報事故等があっても、突然、適用範囲でないと言ってもみ消すおそれもございますので、そもそもISMS、PMS等のISO規格及びJIS規格としての必須ルールとして、契約前にそれらの認証取得者の適用範囲を発注者等のステークホルダーへ開示することを義務化するように、それらの規格を改訂することも経済産業省としてもぜひご検討いただき、ご指導等の善処をしていただければ、有難く存じます。	参考意見として承りました。		
111	一般社団法人 日本画像医療システム工業会	団体	02GL	21	5	5のタイトルと5.1とのタイトルとの間の文章、5.1のタイトルと5.1.1のタイトルとの間の文章を、ぶらさがり段落と呼び、JIS(日本産業規格)等では禁止している構成である。 本ガイドラインは、JISではないが、特に問題ないことはJISの書式、ルールに従うのがいいのではないかと思われます。	行政文書では通例として見られる構成であり、原案のとおりとさせていただきます。		
112	富士通株式会社	団体	02GL	21	5	複数のシステムで構成される医療情報システムにおいて、リスクマネジメントプロセスを個々の事業者に求めることは不適切である。 個人情報保護法「安全管理・確保義務」の規定、厚労省ガイドライン4章、6.2章　により、医療情報システム全体を俯瞰し、リスクマネジメントを行うのは、医療機関の責務である。	医療機関等が、その使用する医療情報システムの全体のリスクマネジメントを行う責務を有しているのはご認識のとおりですが、個々の医療情報システムを提供する対象事業者に対して、提供するその医療情報システムについて、リスクマネジメントプロセスを求めることは適切とは考えております。		
113	HEASNET事務局	団体	02GL	22	5.1.1	"アプリケーションを提供する等により、医療機関との契約もしくは医療機関からの指示の下、情報の中身を意識した情報処理を行う対象事業者においては、～"と修正すべきではないか。	ご認識のとおり、当該記述は、対象事業者が医療機関等の指示等なく独自に情報の中身を把握することは想定しておらず、後述において「医療機関等へ情報提供を求め」ることとしていますので、原案のとおりとさせていただきます。		
114	一般社団法人 日本画像医療システム工業会	団体	02GL	22	5.1.1	"アプリケーションを提供する等により、医療機関との契約もしくは医療機関からの指示の下、情報の中身を意識した情報処理を行う対象事業者においては、～"と修正すべきではないか。	ご認識のとおり、当該記述は、対象事業者が医療機関等の指示等なく独自に情報の中身を把握することは想定しておらず、後述において「医療機関等へ情報提供を求め」ることとしていますので、原案のとおりとさせていただきます。		
115	個人	個人	02GL	22	5.1.1	「医療情報安全管理ガイドライン」の6.2.3 リスク分析にも脅威が挙げてあるので、引用すべきである。	本記述は、医療情報システムの提供上の代表的な脅威を抽出したものであり、原案のとおりとさせていただきます。		
116	HEASNET事務局	団体	02GL	24	5.1.2	"顕在率"ではなく"顕在化率"の方が適しているのではないか。	ご指摘を踏まえて修正いたします。	「顕在率」	「顕在化率」
117	一般社団法人 日本画像医療システム工業会	団体	02GL	24	5.1.2 図5-2	「図 5-2 にリスクレベルに応じたリスク対応の例を示す。」⇒「図 5-2 に影響度と顕在率に応じた選択肢の考え方を示す。」	ご指摘を踏まえて修正いたします。	「図 5-2 にリスクレベルに応じたリスク対応の例を示す。」	「図 5-2 に影響度と顕在化率に応じた選択肢の考え方を示す。」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
118	一般社団法人 日本画像医療システム工業会	団体	02GL	24	5.1.2	”顕在率”ではなく”顕在化率”の方が適しているのではないか。	ご指摘を踏まえて修正いたします。	「顕在率」	「顕在化率」
119	一般社団法人 日本画像医療システム工業会	団体	02GL	24	5.1.2	本文中には、情報流の分類によってリスク影響度が異なる旨の記載がありますが、分類例では、それに触れていません。また、以降の章でも、情報流の分類によってリスク影響度が異なる旨の記載がありません。例えば5.1.4. リスク対応の選択肢の選定 (2)リスク回避に、「対象事業者は、影響度及び顕在率ともに極めて高いリスクについては」という記載がありますが、情報流の違いによる影響度の違いの記載はありません。	情報流の分類によるリスクへの影響度の具体例は「5.2.1. リスクアセスメント」の「(3) リスク特定・リスク分析・リスク評価における成果物の作成」にて述べております。		
120	一般社団法人 日本画像医療システム工業会	団体	02GL	25	5.1.4	現行の総務省ガイドライン発行時のパブコメ回答(2018.7)No.38において、 「本ガイドラインはクラウド事業者が受託した医療情報の安全確保を目的としているため、 クラウド事業者の判断でリスク受容は適当ではない。 クラウド事業者にたい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。 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が可能」とあります。 従って、上記認識に変更が無いならば、記載の追加等の見直しを求めます。	FAQにより整理しましたので、ご参照ください。		
121	HEASNET事務局	団体	02GL	26	5.1.4(3)、(4)	現行の総務省ガイドライン発行時のパブコメ(2018.7)のNo.38 「リスク低減策だけでなく、リスク移転、リスク受容等を選択可能の明示を」に対しての回答において、 「本ガイドラインはクラウド事業者が受託した医療情報の安全確保を目的としているため、クラウド事業者の判断でリスク受容は適当ではない。クラウド事業者にたい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。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が可能」とある。 従って、この認識に変更が無いならば、(3)リスク移転、(4)リスク保有は、事業者が独自判断で医療情報の情報流においてリスク移転並びにリスク保有が出来る様にも読めるため、本文の内容を、下記とするべきではないか。 (3)リスク移転 「リスク低減をしたとしても、顕在化率の低減は可能だが、影響度の低減は困難であるリスクについては、リスク移転を検討することが有効である。ただし、残留リスクの移転を情報流としての他事業者への委託等は、利用者である医療機関等の承認事項であるため、事前に医療機関等への説明・承認・契約が必要である。」 (4)リスク保有 「対象事業者は、リスクアセスメントの結果、リスク低減等のリスク対応を検討した上で、残存するリスクについては、当該リスクを認識した上でリスク保有を検討すること。ただし、残留リスクの保有については、利用者である医療機関等の承認事項であるため、事前に医療機関等への説明・承認・契約が必要である。」	FAQにより整理しましたので、ご参照ください。		
122	一般社団法人 日本画像医療システム工業会	団体	02GL	26	5.1.4(3)	文が分かりづらいため、下記のように修正してはどうか。(”顕在率”→”顕在化率”も反映) ”リスク低減を行った結果、顕在化率の低減は可能だが影響度の低減は困難なリスクについては、リスク移転を検討することが有効である。”	ご指摘を踏まえて修正いたします。	「リスク低減をしたとしても、顕在率の低減は可能だが、影響度の低減は困難であるリスクについては、リスク移転を検討することが有効である。」	「リスク低減を行った結果、顕在化率の低減は可能だが影響度の低減は困難なリスクについては、リスク移転を検討することが有効である。」
123	グーグル・クラウド・ジャパン合同会社	団体	02GL	27-28	5.1.5	SSL-VPNを利用する場合、クライアントSSL証明書を利用することが必須かのように読み取れますが、その様な趣旨では無いという理解で宜しいでしょうか。	本ガイドラインは、「医療情報システムの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する」という方針に基づき、可能な限り一律の要求事項を排すよう努めていますが、医療情報システム特有の考慮事項として必要と考えられる個別の要求事項については、これを記述しているものです		
124	アマゾン ウェブ サービス ジャパン株式会社	団体	02GL	27	5.1.5（1）（ア）	別紙2に基づく対策項目は、実務に対する参考項目であることを明らかにするべきであり、本ガイドライン遵守のための必須要件であるかのように記述することは避けるべきと考えます。	FAQにより整理しましたので、ご参照ください。		
125	個人	個人	02GL	27	5.1.5	「6. 医療分野における制度上の要求事項」に関するリスクも整理すべきである。	リスクマネジメントによらず、およそ医療分野において法令等で作成・保存が義務付けられた医療情報の安全管理にあたり、全ての対象事業者に対し一律の対応が求められる事項については、「6. 医療分野における制度上の要求事項」で対応することと整理しています。		
126	HEASNET事務局	団体	02GL	28	5.1.5(1)(イ)③	医療情報の機密性の高さや攻撃手法の高度化に対応するために、オープンネットワークが第一選択肢であるように見え、注釈21がHTTPS、SSL-VPNの内容のみであるため、クローズドネットワークの採用や、オープンネットワークでの対応策の例示としてIPsec等を記載すべきではないか。	ご指摘を踏まえて修正いたします。	「医療情報の機密性の高さや攻撃手法の高度化に鑑み、オープンなネットワークを介して接続を行う際は、様々な攻撃を想定した上で、適切な暗号化手法を選択すべきである。」	「対象事業者は、提供するサービスに応じ、クローズドネットワークを含むネットワーク経路を適切に選択することが必要である。医療情報の機密性の高さや攻撃手法の高度化に鑑みた上で、クローズドネットワークを採用せず、オープンなネットワークを介して接続を行う際は、様々な攻撃を想定した上で、適切な暗号化手法 を選択すべきである。」
127	一般社団法人 日本画像医療システム工業会	団体	02GL	28	5.1.5(1)(イ)③	医療情報の機密性の高さや攻撃手法の高度化に対応するために、オープンネットワークが第一選択肢であるように見え、注釈21がHTTPS、SSL-VPNの内容のみであるため、クローズドネットワークの採用や、オープンネットワークでの対応策の例示としてIPsec等を記載すべきではないか。	ご指摘を踏まえて修正いたします。	「医療情報の機密性の高さや攻撃手法の高度化に鑑み、オープンなネットワークを介して接続を行う際は、様々な攻撃を想定した上で、適切な暗号化手法を選択すべきである。」	「対象事業者は、提供するサービスに応じ、クローズドネットワークを含むネットワーク経路を適切に選択することが必要である。医療情報の機密性の高さや攻撃手法の高度化に鑑みた上で、クローズドネットワークを採用せず、オープンなネットワークを介して接続を行う際は、様々な攻撃を想定した上で、適切な暗号化手法 を選択すべきである。」
128	個人	個人	02GL	28	5.1.5	これについてであるが、VPN使用における暗号化のみでは事業者又はその関係者による盗聴・改竄を防ぐ事が困難である事から、VPNを使用する場合であっても更にその上でHTTPS等のVPN事業者が関与出来ない様な暗号化通信を行うべきである事について、注意していただきたい。 (SSL-VPNの使用については脚注での注意がなされているが、L2TP/IPsec等方式を含めた全てのVPNについて、VPN提供事業者によっての暗号化のみでは、そのVPN提供事業者及びその関係事業者による盗聴・改竄に対して脆弱である事から(VPN提供事業者等が何と主張していたとしても、である。(言葉だけならいくらでも自らが不正を全く行わない者達であると主張する事が出来るのである。))、自らが、VPN用の暗号化以外での、TLS等による、自ホスト−相手ホストとのP2Pの形の暗号化方式での暗号化通信を行う事とするよう、注意を促していただきたい。)	FAQにより整理しましたので、ご参照ください。		
129	個人	個人	02GL	28	5.1.5	これについては賛成であるが、加えて、同項で、通信時においてはその通信プロトコルについて、いわゆる「素」のプロトコルについて用いないように注意するよう促していただきたい。 WEP、WPA、WPA2、WPA3については脆弱性が幾度となく報告されているが、無線LANシステムが提供する暗号化だけでよしとするのは、問題があるものであるので(それらは、基本的には、他の無線局と通信が混線しないように用いられるものであると割り切って使うものと見なすべきであると考える。)、通信コンテンツについてはWPAシリーズ等が使用している暗号化に加えての暗号化通信が行われるように促していただきたい。 (WPA2等による通信の暗号化があったとしても、HTTPやTELNET(あるいは暗号化されていない他一般的なプロトコル)ではなく、HTTPSやSSHを用いるようにせよ、という事である。SIerによっては通信において独自のプロトコル(あるいは暗号化されていない一般的なプロトコル)を用いて端末−サーバとの通信を行わせたりする事があったりするが、その様な場合はSSHによっての暗号化及びトンネリングを行っての通信を行わせる形とするよう、注意を行っていただきたい。) (なお、基本的には、SSHによっての暗号化通信とトンネリングが常時なされるようにするのが適切ではないかと考える。 HTTPSでの通信も含めて、全ての外部との通信がSSHトンネリングによってなされると、面倒が無くてよいのではないかと考える。)	FAQにより整理しましたので、ご参照ください。		
130	一般社団法人日本医療情報学会事務局	団体	02GL	28	5．1．5.（イ）①	「多要素認証を可能な限り早期に採用すべきである。」を「可能な限り安全性の高い認証手段を導入すべきである。」と変更し、脚注20を削除。もし多要素認証の文章を残すのであれば、脚注20を、「医療情報安全管理ガイドライン第5版では、公表10年後に多要素認証を「最低限のガイドライン」とすることを謳っている。」と変更。	ご指摘を踏まえ、注釈については修正させていただきます。	脚註20 「医療情報安全管理ガイドライン第 5 版の公表（平成 29 年 5 月）から約 10 年後に医療情報安全管理ガイドラインの「C.最低限のガイドライン」となることが想定されている。」	脚註23 「医療情報安全管理ガイドラインでは、第5 版の公表（平成29年5月）から約10 年後を目途に、2要素認証の採用を「C.最低限のガイドライン」とすることが想定されている。」
131	一般社団法人日本医療情報学会事務局	団体	02GL	28	5．1．5.（イ）②	法定保存年限の根拠を脚注に追加(提供ソフトウェアが医療機器プログラム(特定保守管理医療機器)に該当する場合は、演算ログがGVP省令第16条に定める安全確保業務に係る記録の対象になり、使用終了後15年間の保存義務が課せられることなど)。	個別の医療情報の法定保存年限については、それぞれの根拠法令における法定保存年限をご確認ください。		

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
132	一般社団法人日本医療情報学会事務局	団体	02GL	28	5．1．5.（イ）③	「オープンなネットワークを介して接続を行う際は」を削除し、脚注21を削除。もし脚注21を削除できないのであれば、第一文を「（主語なし）…行うこと」から「医療情報完全管理ガイドラインは、…行うことを求めている。」と変更。	ご指摘を踏まえ、注釈については修正させていただきます。	「HTTPS接続においては、TLS の設定はサーバ/クライアントともにCRYPTRECが定める「SSL/TLS 暗号設定ガイドライン（第2.0版）平成30年5月8日」（以下、「SSL/TLS暗号設定ガイドライン」という。）に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと。また、医療情報安全管理ガイドラインは、SSL-VPNを原則として利用しないよう求めている。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。」	「医療情報安全管理ガイドラインでは、専用線、公衆網、閉域IP通信網、IPsecを用いたVPN、HTTPSによる暗号化等が例示されている。そこでは、HTTPS接続においては、TLS の設定はサーバ/クライアントともにCRYPTRECが定める「SSL/TLS 暗号設定ガイドライン（第2.0版）平成30年5月8日」（以下、「SSL/TLS暗号設定ガイドライン」という。）に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと、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、そして、IPsecを用いる場合は、IKEを組み合わせる等して、確実にその安全性を確保するように求めている。」
133	一般社団法人 日本画像医療システム工業会	団体	02GL	29	5.1.5(3)	対象事業者が医療機関に求める内容を検討し、それでも対象事業者自身で許容できないリスクが残存する場合は、そのサービスは破綻していると考えられるため、下記のように修正してはどうか。これに伴い、図の5-1を修正すべき。 修文案:リスク評価の結果、残存するリスクの評価結果において対象事業者として許容できないものが存在しないようにすること。	FAQにより整理しましたので、ご参照ください。		
134	株式会社セールスフォース・ドットコム	団体	02GL	29	5.1.5	対象事業者がクラウドサービス事業者である場合は「リスク対応一覧」を医療機関毎に文書化する方法によらず、対象事業者が医療機関へ提供する、当該サービスの第三者による監査報告書等を活用するように規定すべきである。	クラウドサービス事業者が、そのサービスを特定の顧客向けでなく、マルチテナント形式によって広く顧客に対し同一構成のサービスを提供していてもなお、各医療機関等に対し、文書化したリスク対応一覧を提供する必要性は変わらないものと考えます。		
135	(株)神戸デジタル・ラボセキュリティ事業部	団体	02GL	30	5.1.6 （1）	・意見内容3 「5.1.6.リスクコミュニケーション」、「（1）医療機関等とのリスクコミュニケーションの実施」の以下の項目に追記する。 【追記前】 「なお、その際には、対象事業者は、医療機関等が容易に理解可能となるよう内容を工夫する等、適切に共通理解を得ること」 【追記後】 「なお、その際には、対象事業者は、医療機関等が容易に理解可能となるよう内容を工夫する、医療機関等から開示要求のあった情報を開示する等、適切に共通理解を得ること」	ご意見につきましては、今後の取組の参考とさせていただきます。		
136	HEASNET事務局	団体	02GL	30	5.1.6(2)	サービス仕様適合開示書と重複する内容もあることから、表4-1の医療機関等へ情報提供すべき項目との関係性も示したほうが理解しやすいのではないか。 運用管理規定：別紙1、I.参考例編（サービス仕様適合開示書）1. （ア）：（1）①、（2）⑤、⑮(特に(a)) （イ）：（1）②、（2）⑥ （ウ）：（2）⑦ （エ）：（2）⑧ （オ）：（2）⑨ （カ）：（2）⑩ （キ）：医療情報と個人情報の違いがあるが（2）⑪ （ク）：（2）⑫ （ケ）：（2）⑬ （コ）：（2）⑭	ご指摘を踏まえて修正いたします。	（追記）	（別紙1 I.参考例編（サービス仕様適合開示書）の(1)及び(2)に、提供事業者ガイドライン記載箇所との関連を追記）
137	一般社団法人 日本画像医療システム工業会	団体	02GL	30	5.1.6 脚注22	「公開」⇒「開示」 でしょう。	ご指摘を踏まえて修正いたします。	「その分析途中についても情報を公開し」	「その分析途中についても情報を開示し」
138	一般社団法人 日本画像医療システム工業会	団体	02GL	30	5.1.6	“後述の運用管理規定” → ”後述の運用管理規程”	ご指摘を踏まえて修正いたします。	「後述の運用管理規定」	「後述の運用管理規程」
139	一般社団法人 日本画像医療システム工業会	団体	02GL	30	5.1.6	”文書・規定の作成” → ”文書・規程の作成”	ご指摘を踏まえて修正いたします。	「文書・規定の作成」	「文書・規程の作成」
140	一般社団法人 日本画像医療システム工業会	団体	02GL	30	5.1.6(2)	サービス仕様適合開示書と重複する内容もあることから、表4-1の医療機関等へ情報提供すべき項目との関係性も示したほうが理解しやすいのではないか。 運用管理規定：別紙1、I.参考例編（サービス仕様適合開示書）1. （ア）：（1）①、（2）⑤、⑮(特に(a)) （イ）：（1）②、（2）⑥ （ウ）：（2）⑦ （エ）：（2）⑧ （オ）：（2）⑨ （カ）：（2）⑩ （キ）：医療情報と個人情報の違いがあるが（2）⑪ （ク）：（2）⑫ （ケ）：（2）⑬ （コ）：（2）⑭	ご指摘を踏まえて修正いたします。	（追記）	（別紙1 I.参考例編（サービス仕様適合開示書）の(1)及び(2)に、提供事業者ガイドライン記載箇所との関連を追記）
141	株式会社セールスフォース・ドットコム	団体	02GL	30	5.1.6	「本ガイドライン及び医療情報安全管理ガイドラインの遵守」 「個人情報保護法やその他最新の関連法令等の遵守」を削除もしくは、運用管理規定の適用範囲を明確にしていただきたい。	対象事業者が、医療情報システムを提供するに際しては、本ガイドライン及び医療情報安全管理ガイドラインの遵守や個人情報保護法やその他最新の関連法令等の遵守等が求められるものであり、その旨が運用管理規定に規定されることは必要と考えます。		
142	株式会社セールスフォース・ドットコム	団体	02GL	30	5.1.6	クラウドサービス事業者のサービスにおいては責任共有モデルの考え方に基づき、医療機関等の環境を含めた運用管理規定の作成は必ず対象事業者の担当となるとは限らず、医療機関等が自ら全体的な運用管理規定の作成を行う場合が適切であるケースや、両者のコラボレーション作業となるケースが想定される。したがって、一律に対象事業者が運用管理規定を文書化するという表現に関して、運用管理規定の文書化を行う者はケース・バイ・ケースでの取り決めとなるよう、(1)医療機関等とのリスクコミュニケーションの実施, (2)文書・規定の作成（ア）～（コ）の各項について記述の見直しを頂きたい。	本ガイドラインでは、対象事業者は、自らが提供する医療情報システムの安全管理に関し、医療機関との共通理解を形成するために医療機関等に対して必要な情報を提供した上で、医療機関等との役割分担等について医療機関等と合意形成を図り、その結果は運用管理規程等により文書化することを求めています。クラウドサービス事業者が、マルチテナント形式で1つのサービスを多数の顧客へ共通的に提供するに際しても、上記のリスクマネジメントのプロセスは必要と考えます。なお、医療機関等が最終的に全体的な運用管理規程作成を行う場合や、医療機関等と対象事業者の合意形成プロセスの結果、医療機関等において修正がなされる場合があることは否定されません。		
143	一般社団法人 日本画像医療システム工業会	団体	02GL	31	5.1.6(2)（ウ）	契約書の取り扱いを運用管理規定に含めることになるように見えるため、下記の修正を行ってはどうか。 修文案：対象事業者は、契約書や運用管理規程を含むマニュアル等の管理方法として、必要に応じて速やかに内容を確認できるようにすること。また、文書の不正な閲覧・操作をアクセス制限等により防止することを運用管理規程に含め、第三者による不正な閲覧・操作を防止すること。	ご指摘を踏まえて修正いたします。	「対象事業者は、契約書や運用管理規程を含むマニュアル等の管理方法として、必要に応じて速やかに内容を確認できるようにするほか、アクセス制限により第三者によるこれら文書の不正な閲覧・操作を防止することを運用管理規程に含めること。」	「対象事業者は、契約書や運用管理規程を含むマニュアル等の管理方法として、必要に応じて速やかに内容を確認できるようにすること。また、文書の不正な閲覧・操作をアクセス制限等により防止することを運用管理規程に含め、第三者による不正な閲覧・操作を防止すること。」
144	一般社団法人 日本画像医療システム工業会	団体	02GL	31	5.1.6(2)（エ）	本項目の機器等は、サービスを実施する際に必要な端末等の機器を指していると考えられるため、対象を明確にしてはどうか。仮にサービスを構築しているマシン等を指す場合は、クラウド等を想定すると台帳管理を行うことは困難であると考える。 修文案：「機器等を用いる場合」→「サービスを実施する際に必要なモバイル端末などの機器等を用いる場合」	ご認識のとおりですが、原案にて理解可能であり、原案のとおりとさせていただきます。		
145	一般社団法人 日本画像医療システム工業会	団体	02GL	31	5.1.6(2)（ケ）	記載内容が分かりにくいため、下記のように修正してはどうか。 修文案：なお、医療機関等への医療情報システム提供にあたり、他社が提供する医療情報システムを利用する場合においても、対象事業者として医療情報システムに対する監査の方針や内容もしくは、監査に代替する対応についても運用管理規程に含めること。	いただいた修文案では、原案と趣旨が異なるように読めるため、原案のとおりとさせていただきます。		
146	一般社団法人 日本画像医療システム工業会	団体	02GL	32	5.2	5.2は、“実施例”のため、本文ではなく、付録等にもっていたほうが読みやすくなると思われます。	本節は、5.1の内容をより理解しやすくなるよう実施例を用いたものであり、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	パート	意見	方針・コメント	修正内容	
								原案	修正案
147	グーグル・クラウド・ジャパン合同会社	団体	02GL	32	5.1.6	上記4）と同様に、個人医療情報の格納における記憶媒体の利用は、可能な限り避けるべきと考えます。	「運用管理規定に含める事項」における「医療情報を格納する記憶媒体の管理方法」とは、小型半導体メモリの利用に関わらず、個人情報を格納する記憶媒体の管理方法として、保管や取扱いの方法及び保管や取扱いに係る履歴の記録について運用管理規程に含めることを求めるものであり、必要な項目であると考えます。		
148	グーグル・クラウド・ジャパン合同会社	団体	02GL	33–37	5.2.1 図5–3～5–7	遠隔地と対象事業者DC間のデータのやり取りにテープ媒体を用い、搬送業者が同媒体を搬送する様なイメージがありますが、セキュリティが担保された通信回線やネットワークを介したデータのやり取りに限定すべきと考えます。	医療情報システム提供上の代表的な脅威にも記述があるように、物理媒体によるデータ搬送については、そういったリスクが存在することはご指摘のとおりですが、本ガイドラインにおいては、対象事業者は、自らが提供する医療情報システムの安全管理に関しリスクマネジメントを行い、医療機関との共通理解を形成するために医療機関等に対して必要な情報を提供した上で、医療機関等との役割分担等について医療機関等と合意形成を図ることとしております。		
149	グーグル・クラウド・ジャパン合同会社	団体	02GL	34	5.2.1 図5–4	上記記載はクラウドサービスの仮想マシンも含まれると記載されていますが、場所についてはどこまで明確すべきかの目安（国、あるいは複数の地域にまたがるサービスの場合は地域など）をお示し頂ければ幸いです。	「5.2.1. リスクアセスメント、(1)リスク特定における医療情報システムの全体構成図の作成」においては、医療情報システムの全体構成図の作成を通じて、情報流及びリスクを網羅的に洗い出すように述べており、その過程で医療情報システムの構成要素は、可能な限り詳細に明らかにすることが望ましいというのが基本的な考えとなり、適切にリスク分析できる程度まで詳細化されているべきと考えます。		
150	一般社団法人 日本画像医療システム工業会	団体	02GL	36	5.2.1	改行位置、インデントが適切でないように思えます。2行目の開始の“媒体で」”が1行目から続いているので、その上とインデントを合わせる。さらに、その次の行の図5-6の前の“(”が前の行になってしまっている。	ご指摘を踏まえて修正いたします。	人が扱う機器や記憶媒体における情報の処理を、「誰が」、「どこの」、「どの機器や記憶媒体で」、「何を」、「どうするか」の切り口で可能な限り明らかにする（図 5-6）。人が扱う機器や記憶媒体としては、情報の閲覧・操作を行うための端末や	（改行位置等を修正） 人が扱う機器や記憶媒体における情報の処理を、「誰が」、「どこの」、「どの機器や記憶媒体で」、「何を」、「どうするか」の切り口で可能な限り明らかにする（図 5 6）。人が扱う機器や記憶媒体としては、情報の閲覧・操作を行うための端末や
151	一般社団法人 日本画像医療システム工業会	団体	02GL	36	5.2.1	“患者が、待合室の、問診用タブレットで、患者情報等を、閲覧・操作する”とあるが、読点(“、”)が多すぎる。さらに、文章で終わっているので最後に句点(。) (変更案) 患者が、待合室の問診用タブレットで、患者情報等を閲覧・操作する。 通信回線事業者が、対象事業者DCと医療機関等との間の閉域網VPNで、アプリケーション提供に係る情報を転送する。	手順3の「誰が」、「どこの」～という事前の記述に揃えた書き方となっており、原案のとおりとさせていただきます。		
152	一般社団法人 日本画像医療システム工業会	団体	02GL	40	5.2.1.(3)	脅威が顕在化した場合のリスクを特定”は、文章が不自然です。 “脅威を検討し、リスクを特定”とか、単純に”リスクを特定“のが適切な文章に思えます。	ご指摘を踏まえて修正いたします。	「脅威が顕在化した場合のリスクを特定」	「脅威の顕在化を想定して特定したリスク」
153	個人	個人	02GL	41	P41	2カラム目の脅威と特定したリスクの内容と異なる。整合をとるべきである。	ご指摘を踏まえて修正いたします。	「アプリケーション提供に係る情報を電子媒体へ不正に複製され…」	「アプリケーション提供に係る情報の改ざん・破壊が生じる」
154	個人	個人	02GL	44	6.1	「国内法の執行の及び範囲」というのは、日本の行政庁と執行協力がある国や地域も含むのか？	本規定の趣旨は、医療機関等は調査機関等の検査に対し、適切かつ円滑に対応できるように求めるものです。		
155	個人	個人	02GL	44	6.1	「医療情報及び当該情報に係る医療情報システムが国内法の執行の及ぶ範囲にあることを確実とすること。」というのは、つまり、相互認定がなされた後のEUにすら医療情報等は保存できないということか？この点について、個人情報保護委員会とは協議したのか？	本記述は、法令で定められた医療機関等に対する義務や行政手続の履行を確保するために必要と認められたものであり、個人情報保護委員会との協議も必要ありません。		
156	一般社団法人 日本画像医療システム工業会	団体	02GL	44	6	タイトルが“医療分野における制度～”となっているが、あくまで、本書は、”医療情報“に関係する部分だけである。含まれないものとして、薬機法への対応。これは、医療機関等ではなく、事業者が気をつけるべき内容。 タイトルを“医療分野における**医療情報に関する**制度～”に修正したほうがいいと考えます。	ご指摘を踏まえて修正いたします。	「医療分野における制度上の要求事項」	「制度上の要求事項」
157	一般社団法人 日本画像医療システム工業会	団体	02GL	44	6	6のタイトルと6.1とのタイトルとの間の文章を、ぶらさがり段落と呼び、JIS(日本産業規格)等では禁止している構成である。本ガイドラインは、JISではないが、特に問題ないことはJISの書式、ルールに従うのがいいのではないかと思われます。	行政文書では通例として見られる構成であり、原案のとおりとさせていただきます。		
158	一般社団法人 日本画像医療システム工業会	団体	02GL	44	6.2	下記の通知が記載されていますが、通知番号等と通知名称とはあっていますか。 「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。 下記の間違いでは。 「「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」（平成 28 年 3 月 31 日付け医政発 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。	ご指摘を踏まえて修正いたします。	「「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。」	「「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 30 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」
159	一般社団法人 日本画像医療システム工業会	団体	02GL	44	6.2	施**工**通知→施**行**通知	ご指摘を踏まえて修正いたします。	「施工通知」	「施行通知」
160	グーグル・クラウド・ジャパン合同会社	団体	02GL	44	6.1	削除、若しくは「…確保するために、適用を受ける法令を調査し、執行を受けた場合の対応を文書化することが望ましい」との内容に変更頂ければ幸いです。なお、データが一時的に国外にて処理され、処理結果が日本に保存されることは問題ないと考えて良いでしょうか？例えば、AIモデル作成のためのデータ保存と機械学習処理を一時的に海外にて実行し、学習の結果生成されたAIモデルは日本国内に保存し利用する、というケースも有り得るかと存じます（海外で機械学習のために使用したデータは、学習終了後に削除）。	本記述は、法令で定められた医療機関等に対する義務や行政手続の履行を確保するために必要なものであり、原案のとおりとさせていただきます。		
161	個人	個人	02GL	44	6	６．１「医療情報安全管理ガイドライン」の要求事項を追加し、C項の最低限のガイドライン遵守を記述すべきである。	本ガイドラインでは、医療情報安全管理ガイドラインにおける制度上の要求事項への対応策について、対象事業者は医療機関等に対し別紙2を適宜参照する等して説明すべきとしています。		
162	(株)神戸デジタル・ラボセキュリティ事業部	団体	02GL	45	5.2	・意見内容4 「危機管理対応時のインシデントレスポンス」に関する記載がない。 「5.安全管理のためのリスクマネジメントプロセス」の中に記載するか、「5.安全管理のためのリスクマネジメントプロセス」の次項目として「6. 危機管理対応時のインシデントレスポンス」を追加する。 内容には以下の項目を記載する。（一般的なインシデントレスポンスの内容に医療機関等との情報連携を追加する方針であるが、例として以下に実施項目を示す） （1）対象事業者が「危機管理対応時」に備えて日頃から実施すべき内容について a.インシデント対応マニュアルの整備 b.インシデント発生時の調査対象情報の収集 ・「危機管理対応時」に調査対象となる情報が収集されているか確認（必要な情報の収集状況、情報を収集する仕組みの有無等 ・上記、調査対象情報の収集の維持管理 ※複数医療機関の情報を取り扱っている場合、個々の医療機関に向けてログ情報等が開示できるように、医療機関単位に情報が抽出できる仕組みや対処手段をあらかじめ用意しなければならない c.インシデント対応訓練の実施 d.インシデント対応について医療機関等と事前の準備内容、インシデント対応の実施内容の合意を得る （2）対象事業者が「危機管理対応時」に実施すべき内容についての記載 a.初期対応 b.本対策 c.事後対応 ※当該医療機関等とは初期対応段階から事後対応まで密に連携をとる。当該医療機関から要求がある場合は、当該医療機関に関わる事故に関する詳細な情報を提供しなければならない。	ご意見につきましては、今後の取組の参考とさせていただきます。		
163	HEASNET事務局	団体	02GL	45	6.3	”上述の電子署名”だと、電子署名の方法を示しているように読み取れるため、”上述の要件、要求事項を満たす電子署名”とすべきではないか。	ご指摘を踏まえて修正いたします。	「上述の電子署名」	「上述の要件、要求事項を満たす電子署名」
164	一般社団法人 日本画像医療システム工業会	団体	02GL	45	6.3	”上述の電子署名”だと、電子署名の方法を示しているように読み取れるため、”上述の要件、要求事項を満たす電子署名”とすべきではないか。	ご指摘を踏まえて修正いたします。	「上述の電子署名」	「上述の要件、要求事項を満たす電子署名」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
165	一般社団法人 日本画像医療システム工業会	団体	02GL	46	用語集	IEC 62853:2018は、用語ではなく参考文献。参考文献を別途、設けて記載するか、あるは、別途Open Systems Dependabiityの用語は説明しているので、削除	ご指摘を踏まえて修正いたします。	IEC 62853:2018 「Open Systems Dependability（開放系総合信頼性）の国際標準。 状況が変化してもシステムが継続してサービスを提供し続けるための要件を記載。 合意形成、説明責任遂行、変化対応、障害対応の４つの観点で構成。」	（削除）
166	一般社団法人 日本画像医療システム工業会	団体	02GL	46	用語集	Open Sytems Dependability →　Open Systems Dependability	ご指摘を踏まえて修正いたします。	「Open Systems Dependability」	「Open Systems Dependability」
167	一般社団法人 日本画像医療システム工業会	団体	02GL	47	用語集	SLAは、JISQ20000-1:2007を参照しているが、JISQ20000-1:2012に更新すべき。 サービス及びサービス目標を特定した，サービス提供者と顧客との間の合意文書(JISQ20000-1:2012)	ご指摘を踏まえて修正いたします。	「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）」	「サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書(JIS　Q　20000-1:2012)」
168	一般社団法人 日本画像医療システム工業会	団体	02GL	47	用語集	可用性、完全性、機密性、脅威、脆弱性、リスクが、JISQ27001を基に定義と記載されているが、27000シリーズでの用語の定義は、JISQ27000なので、それを参照すべき。	ご指摘を踏まえて修正いたします。	「JIS Q 27001」	「JIS Q 27000」
169	一般社団法人 日本画像医療システム工業会	団体	02GL	48	用語集	“「”が1つ多い。日本工業規格は、2019年7月から日本産業規格に名称が変わっています。 “「日本**工業**規格”→ “日本**産業**規格”	ご指摘を踏まえて修正いたします。	「日本工業規格」	「日本産業規格」
170	一般社団法人 日本画像医療システム工業会	団体	02GL	48	用語集	ISO/IECのAnnexSLにより、JISQ31000, JISQ27000のリスクに定義が、ハーモナイズされた。“目的に対して不確かさが与える影響”は、間違い。 (変更案) リスク: 目的に対する不確かさの影響。事象の結果とその起こりやすさ(発生確率)との組み合わせ。	ご指摘を踏まえて修正いたします。	リスク 「目的に対して不確かさが与える影響」	リスク 「目的に対する不確かさの影響。事象の結果とその起こりやすさ(発生確率)との組み合わせ」
171	グーグル・クラウド・ジャパン合同会社	団体	03別紙1	0	全般	IT・クラウドサービスのトランザクション（処理）に関わる全ての関係者に対し、監査認証（例:ISOなど）のレベルを明確にし、そのレベルを維持する必要がある旨示すことで、個々の処理に関わるポイントに焦点を当てる（リソースを掛ける）必要がなくなります。逆に個々の処理に焦点を当ててしまうと、監査認証の価値が下がり、通常の法的な契約交渉がまるで、管理監査になってしまいます（医療機関・クラウドサービスプロバイダー共に、監査資格を有していません）。既にプロバイダーは適切な監査を受け、認証を受けているにも関わらず、“監査のようなもの”に多大な時間を掛けることにより、本来有する価値の提供が難しくなります。また、医療機関側が監査に準ずる業務を行う専門知識とリソースを有しているかも不明です。なお、プロバイダーは内部システムの運用につき、情報機密維持の観点から、顧客とその詳細について共有することを快適と思わない理由があります。よって、プロバイダーは監査資格を有する監査人と監査認証を好む傾向があります。	参考意見として承りました。		
172	個人	個人	03別紙1	0	全般	SLAの内容として以下を追加すべきである。 1）医療情報システムの安全管理の妥当性について、対象事業者内部の独立した監査部門や第三者機関評価の状況 2）医療情報を取り扱う事業者として情報セキュリティに係る公的な第三者認証の取得状況 3）医療機関等へ対応を求める安全管理項目（重要事項説明書） 4）想定したリスク環境、リスク分析とリスク対応一覧表	SLAは参考例です。ご指摘の項目についてはガイドラインで合意すべき項目となっています。SLAは、各社が提供される医療情報システムに応じて適宜修正し、医療機関等の合意形成に使用されるものと考えています。		
173	個人	個人	03別紙1	2	Ⅱ.3.1	「提供事業者ガイドライン」とあるが「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」の略語と思われるが本文上にその定義がないので正式名称を使用すべきである。	ご指摘を踏まえ修正いたします。	「提供事業者ガイドライン」	「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」
174	個人	個人	03別紙1	4	Ⅰ.1	「外部保存を受託する事業者の選定にあたり最低限確認する」とあるのは 「医療情報を取り扱う情報システム・サービスの事業者の選定にあたり最低限確認する」とした方が良い。	ご指摘を踏まえ修正いたします。	「外部保存を受託する事業者の選定にあたり最低限確認する」	「医療情報を取り扱う情報システム・サービスの事業者の選定にあたり最低限確認する」
175	グーグル・クラウド・ジャパン合同会社	団体	03別紙1	5,6	Ⅰ.1.(2).④	こちら④、⑨の内容の違いをご教示頂きたく存じます。	ガイドラインの「表4−1 医療機関等へ情報提供すべき項目」をご参照ください。		
176	一般社団法人 日本画像医療システム工業会	団体	03別紙1	7	Ⅰ.1.(2).⑮	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【厚生労働省】(例)と記載がある。例ではあるが、発行元は、個人情報保護委員会と厚生労働省。改正個人情報保護法に合わせて、従来のガイドラインを個人情報保護委員会も含めて見直しを実施してガイダンスにしている。	ご指摘を踏まえ修正いたします。	「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【厚生労働省】」	「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【厚生労働省・個人情報保護委員会】」
177	グーグル・クラウド・ジャパン合同会社	団体	03別紙1	7	Ⅰ.1.(2).⑪	当該部分の削除もしくは、P.6⑧機器等を用いる場合の機器等の管理方法に吸収頂きたく存じます。	本ガイドラインにおいては、対象事業者は、自らが提供する医療情報システムの安全管理に関しリスクマネジメントを行い、医療機関との共通理解を形成するために医療機関等に対して必要な情報を提供した上で、医療機関等との役割分担等について医療機関等と合意形成を図ることとしております。		
178	グーグル・クラウド・ジャパン合同会社	団体	03別紙1	7	Ⅰ.1.(2).⑪	当該部分の削除又は、「適正な法執行に基づく日本国からの要請を排除しない国・地域に設置する」へのご変更をお願い申し上げます。	本ガイドラインにおいては、法令で定められた医療機関等に対する義務や行政手続の履行を確保するために、医療情報及び当該情報に係る医療情報システムが国内法の執行の及ぶ範囲にあることを確実とすることを求めているものです。		
179	一般社団法人 日本画像医療システム工業会	団体	03別紙1	8	Ⅰ.1.(2).⑮.(b).(ア)	“通信の相手先が正当であることを認識するための相互認証を**おこなうこと**”と記載あるが、医療情報安全管理ガイドラインの表記に合わせて“**行うこと**”に変更。	ご指摘を踏まえ修正いたします。	「おこなう」	「行う」
180	一般社団法人 日本画像医療システム工業会	団体	03別紙1	9	Ⅰ.1.(2).⑮.(b).(イ)	“医療情報安全管理ガイドライン7.2 C.最低限のガイドライン”と記載あるが、医療情報安全管理ガイドライン7.2(P104)によると、D.推奨されるガイドラインである。	ご指摘を踏まえ修正いたします。	「7.2 C.最低限のガイドライン」	「7.2 D.推奨されるガイドライン」
181	一般社団法人 日本画像医療システム工業会	団体	03別紙1	10	Ⅰ.1.(2).⑮.(b).(ウ)	医療情報安全管理ガイドライン7.3 C.最低限のガイドライン “(4) 媒体・機器・ソフトウェアの**整合性不備による**復元不能の防止”と記載あるが、医療情報安全管理ガイドラインの表記に合わせて“**不整合による情報の**”に変更。	ご指摘を踏まえ修正いたします。	「(4) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止」	「(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止」
182	一般社団法人 日本画像医療システム工業会	団体	03別紙1	10	Ⅰ.1.(2).⑮.(b).(ウ)	医療情報安全管理ガイドラインには、ネットワークを通じて医療機関等の外部に保存する場合の最低限のガイドライン、推奨されるガイドラインの両方あるが、本書に記載されていない。 最低限のガイドライン （1） データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと （2） ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと 推奨されるガイドライン （3） ネットワークや外部保存を受託する機関の設備の互換性を確保すること	別紙1のサービス仕様適合開示書はあくまで参考例です。また、項目は厚生労働省の医療情報安全管理ガイドラインではなく、本ガイドラインに沿ったものとなっております。		
183	一般社団法人 日本画像医療システム工業会	団体	03別紙1	10	Ⅰ.1.(2).⑮.(c)	誤植　“サービス**に**提供に際して”→“サービス**の**提供に際して”	ご指摘を踏まえ修正いたします。	「サービスに提供に際して法令で定められた記名・押印を電子署名で行う文書」	「サービスの提供に際して法令で定められた記名・押印を電子署名で行う文書」
184	一般社団法人 日本画像医療システム工業会	団体	03別紙1	10	Ⅰ.1.(2).⑮.(c)	(c)のタイトルとその下の節の(ア)のタイトルが全く同じでかつ、(c)の下のは、(ア)しか存在しない。このため、(ア)のタイトルは不要	ご指摘を踏まえ修正いたします。	「(ア) 法令で定められた記名・押印を電子署名で行うことについて」	（削除）
185	一般社団法人 日本画像医療システム工業会	団体	03別紙1	10	Ⅰ.1.(2).⑮.(d)	誤植　“サービス**に**提供に際して”→“サービス**の**提供に際して”	ご指摘を踏まえ修正いたします。	「サービスに提供に際して処理するその他取扱いに注意を要する文書等」	「サービスの提供に際して処理するその他取扱いに注意を要する文書等」
186	HEASNET事務局	団体	03別紙1	20	Ⅱ.3.1	6．6(3)のタイトルは”運用状況に係る情報提供について”ではないのか。	ご指摘を踏まえ修正いたします。	「6．6(3)(機密保持契約の締結等)」	「6．6(3)(運用状況に係る情報提供について)」
187	一般社団法人 日本画像医療システム工業会	団体	03別紙1	20	Ⅱ.3.1	6．6(3)のタイトルは”運用状況に係る情報提供について”ではないのか。	ご指摘を踏まえ修正いたします。	「6．6(3)(機密保持契約の締結等)」	「6．6(3)(運用状況に係る情報提供について)」
188	一般社団法人 日本画像医療システム工業会	団体	03別紙1	24	3.4	“対象事業者によっては、ISO9001等の認証を取得している場合には、これを取得していることをもって”と記載されているが、ITサービスの品質だと、ISO20000も有名であり、有効である。このため、ISO9001 と併記して、 “ISO9001及び/又はISO20000等の認証”にしたほうがいいのではと思われる。	ご指摘を踏まえ修正いたします。	「ISO9001等の認証」	「ISO 9001及び/又はISO 20000等の認証」
189	HEASNET事務局	団体	03別紙1	25	Ⅱ.3.5	本ガイドラインの正式名称で例示してはどうか。	ご指摘を踏まえ修正いたします。	「医療情報の処理を受託する事業者における安全管理ガイドライン（経済産業省、総務省令和２年３月）」	「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　令和〇年〇月）」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
190	一般社団法人 日本画像医療システム工業会	団体	03別紙1	25	Ⅱ.3.5	より一般的な記載方法の方がいいのではないか。 “平成15年**5月30日**法律第57号”→“平成15年法律第57号”	ご指摘を踏まえ修正いたします。	「個人情報の保護に関する法律（平成15年5月30日法律第57号）」	「個人情報の保護に関する法律（平成15年法律第57号）」
191	一般社団法人 日本画像医療システム工業会	団体	03別紙1	25	Ⅱ.3.5	“医療情報の処理を受託する事業者における安全管理ガイドライン（経済産業省、総務省令和2年3月）” (1) 正式なガイドライン名のがいいのでは。 (2) 令和の前に空白 (3) 省の順序は建制順がいいのでは。 (変更案) “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3月）”	ご指摘を踏まえ修正いたします。	「医療情報の処理を受託する事業者における安全管理ガイドライン（経済産業省、総務省令和2年3月）」	「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　令和〇年〇月）」
192	一般社団法人 日本画像医療システム工業会	団体	03別紙1	25	Ⅱ.3.5	“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（厚生労働省 平成29年5月31日）” (1) 発行年月日間違い (2) 発行者間違い “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（**個人情報委員会**、厚生労働省 平成29年**4**月**14**日）”	ご指摘を踏まえ修正いたします。	「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（厚生労働省 平成29年5月31日）」	「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（個人情報委員会、厚生労働省 平成29年4月14日）」
193	一般社団法人 日本画像医療システム工業会	団体	03別紙1	25	Ⅱ.3.5	“それらのガイドラインに対応する医療機関等が遵守すべき2つのガイドラインについても“とあるが、上記には3つ記載されている。 ・医療・介護関係事業者における個人情報の適切な取扱いのための**ガイダンス**（厚生労働省 平成29年5月31日） ・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（厚生労働省 平成29年5月） ・クラウドサービスにおける情報セキュリティ対策ガイドライン 第2版（総務省 平成30年7月） この中で、医療機関等が遵守すべきは、先頭の2つ、最後の1つは、医療機関等ではなく、クラウド事業者が参考にすべき内容。 また、“2つのガイドライン”となっているが、正確には”ガイダンス“とガイドラインである。 (1) 変更案 それらのガイドラインに対応する医療機関等が遵守すべきガイダンス、ガイドラインの2つについても (2) クラウドサービス”ガイドラインを削除	ご指摘を踏まえ修正いたします。	3.5 準拠する法令・ガイドライン等 ・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（厚生労働省 平成 29 年 5 月 31 日） ・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（厚生労働省 平成29 年 5 月） ・クラウドサービスにおける情報セキュリティ対策ガイドライン 第 2 版（総務省平成 30 年7月） 【本項を定める上での考え方】 「それらのガイドラインに対応する医療機関等が遵守すべき2つのガイドラインについても」	3.5 準拠する法令・ガイドライン等 ・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（個人情報委員会、厚生労働省 平成29年4月14日） ・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（厚生労働省　平成29年5月） （削除） 【本項を定める上での考え方】 「それらのガイドラインに対応する医療機関等が遵守すべきガイダンス、ガイドラインの2つについても」
194	一般社団法人 日本画像医療システム工業会	団体	03別紙1	25	Ⅱ.3.5	本ガイドラインの正式名称で例示してはどうか。	ご指摘を踏まえ修正いたします。	「医療情報の処理を受託する事業者における安全管理ガイドライン（経済産業省、総務省令和 2 年 3 月）」	「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　令和〇年〇月）」
195	個人	個人	03別紙1	25	Ⅱ.3.5	旧ガイドライン2つ残っているので削除すべきである。	ご指摘を踏まえ修正いたします。	3.5 準拠する法令・ガイドライン等 本サービスの提供に当たり、乙は、下記に示す法令及びガイドラインを遵守する。 ・個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号） ・医療情報の処理を受託する事業者における安全管理ガイドライン（経済産業省、総務省令和 2 年 3 月） なお、上記ガイドラインの遵守は、下記のガイドラインに記述された趣旨を理解した上で、実施する。 ・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（厚生労働省 平成 29 年 5 月 31 日） ・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（厚生労働省 平成29 年 5 月） ・クラウドサービスにおける情報セキュリティ対策ガイドライン 第 2 版（総務省平成 30 年7月）	3.5 準拠する法令・ガイドライン等 本サービスの提供に当たり、乙は、下記に示す法令及びガイドラインを遵守する。 ・個人情報の保護に関する法律（平成15年法律第57号） ・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　令和〇年〇月） なお、上記ガイドラインの遵守は、下記のガイダンス及びガイドラインに記述された趣旨を理解した上で、実施する。 ・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（個人情報委員会、厚生労働省 平成29年4月14日） ・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（厚生労働省　平成29年5月） （削除）
196	一般社団法人 日本画像医療システム工業会	団体	03別紙1	26	Ⅱ.3.6	(現状) 業務上知り得た秘密（個人情報を含む）を保護するための守秘義務**規程**を個人情報保護**規程**等で文書化すること (変更案) 業務上知り得た秘密（個人情報を含む）を保護するための守秘義務**規定**を個人情報保護**規程**等で文書化すること	ご指摘を踏まえ修正いたします。	「業務上知り得た秘密（個人情報を含む）を保護するための守秘義務規程を個人情報保護規程等で文書化すること。」	「業務上知り得た秘密（個人情報を含む）を保護するための守秘義務規定を個人情報保護規程等で文書化すること。」
197	一般社団法人 日本画像医療システム工業会	団体	03別紙1	26	Ⅱ.3.6	“再委託事業者**若しくは**サービス提供に際して用いる他の事業者“と記載しているが、”若しくは”ではなく、”**又は**“を使うべき。(JISZ8301等参照)	ご指摘を踏まえ修正いたします。	「再委託事業者若しくはサービス提供に際して用いる他の事業者」	「再委託事業者又はサービス提供に際して用いる他の事業者」
198	一般社団法人 日本画像医療システム工業会	団体	03別紙1	27	Ⅱ.3.7	“厚生労働省ガイドラインでは”としているが、本ガイドライン本書あるいは、本別紙内の適合開示書内では、“医療情報安全管理ガイドライン”と記載している。これに合わせたほうがいい。 “厚生労働省ガイドラインでは”を“医療情報安全管理ガイドラインでは”と修正。 同様にP32, P39, P40, P41, P43, P45, P47, P48, P49, P50等にも“厚生労働省ガイドラインでは”の記載も同様に修正。	ご指摘を踏まえ修正いたします。	「厚生労働省ガイドライン」	「医療情報安全管理ガイドライン」
199	一般社団法人 日本画像医療システム工業会	団体	03別紙1	31	4.1	“乙は、甲の連絡若しくは自己の判断に基づき、”と記載されているが、“若しくは”ではなく、”又は”にすべき。 (参考　JISZ8301)	ご指摘を踏まえ修正いたします。	「乙は、甲の連絡若しくは自己の判断に基づき」	「乙は、甲の連絡又は自己の判断に基づき」
200	一般社団法人 日本画像医療システム工業会	団体	03別紙1	31	4.1	“障害の要因が乙の管理する、機器、アプリケーション等のシステム、ネットワーク、**及び**これに関連するサービス等に起因するもの”と記載されているが、ここでは、”及び”ではなく、“又は”にすべき。機器、システム、ネットワーク、サービスのどれかに起因するときなため。	ご指摘を踏まえ修正いたします。	「障害の要因が乙の管理する、機器、アプリケーション等のシステム、ネットワーク、及びこれに関連するサービス等に起因するもの」	「障害の要因が乙の管理する、機器、アプリケーション等のシステム、ネットワーク、又はこれに関連するサービス等に起因するもの」
201	一般社団法人 日本画像医療システム工業会	団体	03別紙1	41	Ⅱ.5.2	“複数の担当業務若しくは職種毎に“の”若しくは“は、”又は“に修正すべき。 (JISZ8301等参考)	ご指摘を踏まえ修正いたします。	「複数の担当業務若しくは職種毎に」	「複数の担当業務又は職種毎に」
202	一般社団法人 日本画像医療システム工業会	団体	03別紙1	41	Ⅱ.5.2	“複数の担当業務若しくは職種に関するアクセス権限“の”若しくは“は、”又は“に修正すべき。 (JISZ8301等参考)	ご指摘を踏まえ修正いたします。	「複数の担当業務若しくは職種に関するアクセス権限」	「複数の担当業務又は職種に関するアクセス権限」
203	一般社団法人 日本画像医療システム工業会	団体	03別紙1	43	Ⅱ.5.2	“作成責任者若しくは代行取込者”の”若しくは“は、”又は“に修正すべき。 (JISZ8301等参考)	ご指摘を踏まえ修正いたします。	「作成責任者若しくは代行取込者」	「作成責任者又は代行取込者」
204	一般社団法人 日本画像医療システム工業会	団体	03別紙1	44	5.2	“代行操作者用のID及び権限付与が設定できること”は、少し誤解をまねくおそれがある。あたかも、”代行操作のためのID”を設けるようにも読めてしまう。こうするとそのIRを代行操作で使いまわされる可能性もある。IDはあくまで、個人に対して発行し、だれが操作したか明確にわかるようにすべき。 このため、対象の部分を下記のように修正 (変更前) 代行操作者用のID及び権限付与が設定できること (変更案) 代行操作の権限付与が設定できること	ご指摘を踏まえ修正いたします。	「代行操作者用のID及び権限付与が設定できること」	「代行操作の権限付与が設定できること」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
205	一般社団法人 日本画像医療システム工業会	団体	03別紙1	44	Ⅱ.5.2	“具体的な対応の内容としては、原因の究明、警察等への通報、データの回復措置等などが想定される。“と例示されている。例示といえども、一番重要な記載が抜けてしまっている。”被害拡大防止、二次被害防止 “。これを実施するために、状況把握が必要。 (変更前) 具体的な対応の内容としては、原因の究明、警察等への通報、データの回復措置等などが想定される。 (変更案) 具体的な対応の内容としては、**被害状況の把握、被害拡大防止**、原因の究明、警察等への通報、データの回復措置等などが想定される。	ご指摘を踏まえ修正いたします。	「具体的な対応の内容としては、原因の究明、警察等への通報、データの回復措置等などが想定される。」	「具体的な対応の内容としては、被害状況の把握、被害拡大防止、原因の究明、警察等への通報、データの回復措置等が想定される。」
206	一般社団法人 日本画像医療システム工業会	団体	03別紙1	44	Ⅱ.5.2	“不正若しくは過誤による”の”若しくは“は、”又は“に修正すべき。 (JISZ8301等参考)	ご指摘を踏まえ修正いたします。	「不正若しくは過誤による」	「故意又は過失による」
207	一般社団法人 日本画像医療システム工業会	団体	03別紙1	44	Ⅱ.5.2	“不正”若しくは“過誤“と表現しているが、参考にしている医療情報安全管理ガイドライン7.1では、”故意又は過失”と表現している。 不正: 広く法秩序や義務に違反すること。 過誤:あやまち、過失のある過ち 過失:あやまち、注意義務に違反する状態や不注意 ただし、医療情報安全管理ガイドラインでは、“虚偽入力、書換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じる”と説明はあり、操作者が十分注意していても発生する誤りも含めているようにも読める。 このため、参考にしている医療情報安全管理ガイドラインの言葉に合わせて、“故意又は過失”にすべき。	ご指摘を踏まえ修正いたします。	「不正若しくは過誤による」	「故意又は過失による」
208	一般社団法人 日本画像医療システム工業会	団体	03別紙1	45	Ⅱ.5.2	“本項で定める画面につき、“適宜変更を行う。~”と記載されており、もし、”変更”する場合の注意事項は妥当だと思われるが、”変更“が当然のような記載になってしまっている。初期から見読性を確保できていれば、変更がいらないはずであり、変更することを前提とする記載とすべきでない。つまり、下記の変更案のようにするか、これらを削除する。特に誤って確定されないは、見読性に大きく関与するとは思えない。 (変更案) 本項で定める画面について、何かしらの事情で変更する場合、下記に注意する。 - 乙は事前に甲に予告する。 - 乙は、入力結果が誤って確定されない設計を維持する。	ご指摘を踏まえ修正いたします。	「本項で定める画面につき、乙は、予告の上、適宜変更を行う。変更に際して、乙は、入力結果が誤って確定されない設計となることに努める。」	「本項で定める画面について、何かしらの事情で変更する場合、乙は、予告の上、適宜これを行う。変更に際して、乙は、入力結果が誤って確定されない設計となることに努める。」
209	一般社団法人 日本画像医療システム工業会	団体	03別紙1	45	Ⅱ.5.2	“乙は、甲の連絡若しくは自己の判断に基づき、調査し、報告を行う。”と記載されているが、日本語をよりわかりやすくすべき。 (変更案) 乙は、甲**から**の連絡**または**自己の判断に基づき、調査し、**甲への**報告を行う。	ご指摘を踏まえ修正いたします。	「乙は、甲の連絡若しくは自己の判断に基づき、調査し、報告を行う。」	「乙は、甲からの連絡または自己の判断に基づき、調査し、甲への報告を行う。」
210	一般社団法人 日本画像医療システム工業会	団体	03別紙1	47	Ⅱ.5.2	“データの劣化“と多くの場所で使われているが、”データの劣化“は非常にわかりにくい言葉である。”データ“は劣化しない。劣化するのは、媒体、設備等である。さらにデータ形式、プロトコルの更新による過去データの扱い等も注意が必要。データの劣化に関する適切な説明をしてから使うか、使用箇所を適切な言葉に置き換えるべき。医療情報の安全管理ガイドラインでは、”データの劣化”の言葉は使っていない。	ハードウェア的劣化だけでなく、ソフトウェア的劣化を含んでおりますので、原案のとおりとさせていただきます。		
211	一般社団法人 日本画像医療システム工業会	団体	03別紙1	47	Ⅱ.5.2	“~何らかの障害が発生し~データが転送していなかった場合に、その旨を表示する機能を実装する例を~”と記載されているが、データ転送されなかった場合に、転送されなかったを表示することはかなり難しいのではと思われる。転送されたは表示可能、転送されなかったは表示できない。あくまで、転送できなかったことが確認できる機能と表現すべきでは。これにより、データ転送がうまくいったものを表示し、転送がうまくいかなかったものは表示されないことで、転送できなかったことが間接的に確認可能になる。 (変更前) “~何らかの障害が発生し~データが転送していなかった場合に、その旨を表示する機能を実装する例を~” (変更案) “~何らかの障害が発生し~データが転送していなかった場合に、その旨**の確認が可能な**表示**を**する機能を実装する例を~”	通信が確立されなかった場合も含めておりますので、原案のとおりとさせていただきます。		
212	一般社団法人 日本画像医療システム工業会	団体	03別紙1	47	Ⅱ.5.2	“~パターンファイルの更新、**及び**OS**及び**ミドルウェア等のセキュリティパッチ~”と記載あるが、“及び”が階層的に2度使われてしまっている。JISZ8301、法律文書等の記載方法に合わせ、”並びに”、”及び“を適切に使い分けるべき。 (変更案) “~パターンファイルの更新、**並びに**OS**及び**ミドルウェア等のセキュリティパッチ~”	ご指摘を踏まえ修正いたします。	「及びOS及びミドルウェア等のセキュリティパッチ」	「並びにOS及びミドルウェア等のセキュリティパッチ」
213	一般社団法人 日本画像医療システム工業会	団体	03別紙1	49	Ⅱ.5.2	“~機能若しくは手順”の“若しくは”は、”又は“にすべき。 JISZ8301等参照	ご指摘を踏まえ修正いたします。	「機能若しくは手順」	「機能又は手順」
214	一般社団法人 日本画像医療システム工業会	団体	03別紙1	51	Ⅱ.6.1	医療機関等では、医療情報ガイドラインでも明確に“運用管理規程”と呼ぶ文章を要求している。対象事業者では、運用を管理するための規程等は要求されているが、それを、医療機関等と同様に“運用管理規程”としてしまうとさまざまな部分で混乱を招く恐れがある。対象事業者向けに“運用管理規程”以外の適切な用語を定義して、それを一貫して使うように全体を見直したほうがいい。	対象事業者においても運用管理規程という用語は一般的に使われているものと認識しており、原案のとおりとさせていただきます。		
215	一般社団法人 日本画像医療システム工業会	団体	03別紙1	52	6.1	“~情報セキュリティ対策ガイドラインにより、~情報資産の運用管理の文書化が求められている。”と記載されているが、 (1) 情報セキュリティ対策ガイドラインはどのガイドラインを指すか？本別紙、及び本ガイドライン本文では、定義されていない。 ・「ASP・SaaSにおける**情報セキュリティ対策ガイドライン**」(以下、「ASP・SaaSセキュリティガイドライン」という。 ・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**(平成30年7月 総務省) (2) 前記、(1)のどちらかだと仮定しても情報資産の運用管理の文書化の要件が見当たらない。	ご指摘を踏まえ修正いたします。	「また、対象事業者においても、情報セキュリティ対策ガイドラインにより、情報資産の運用管理の文書化が求められる。そこで、これらの規程間の整合を図る必要が生じる。」	「また、対象事業者においても、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5.1.6にもとづく文書化が求められる。そこで、これらの規程間の整合を図る必要が生じる。」
216	一般社団法人 日本画像医療システム工業会	団体	03別紙1	57	6.2	“~必要な説明若しくはこれにかわる資料”の“若しくは”は、“又は”にすべき。JISZ8301等参照。	ご指摘を踏まえ修正いたします。	「必要な説明若しくはこれに代わる資料」	「必要な説明又はこれに代わる資料」
217	一般社団法人 日本画像医療システム工業会	団体	03別紙1	57	6.2	“~必要な説明若しくはこれにかわる資料”の“若しくは”は、“又は”にすべき。JISZ8301等参照。	ご指摘を踏まえ修正いたします。	「必要な説明若しくはこれに代わる資料」	「必要な説明又はこれに代わる資料」
218	一般社団法人 日本画像医療システム工業会	団体	03別紙1	62	6.3	“~乙による感知若しくは甲からの連絡~”の“若しくは”は、“又は”にすべき。JISZ8301等参照。	ご指摘を踏まえ修正いたします。	「乙による感知若しくは甲からの連絡」	「乙による感知又は甲からの連絡」
219	一般社団法人 日本画像医療システム工業会	団体	03別紙1	63	6.3	“~乙による感知若しくは甲からの連絡~”の“若しくは”は、“又は”にすべき。JISZ8301等参照。	ご指摘を踏まえ修正いたします。	「乙による感知若しくは甲からの連絡」	「乙による感知又は甲からの連絡」
220	一般社団法人 日本画像医療システム工業会	団体	03別紙1	65	6.4	“【http://+++.****.jp/-----/(乙の用意するWeb上のページ)】”と例示されているが、例示とはいえ、httpではなく、httpsにしておいたほうがいいのではないか。 他、同様の箇所すべて。	ご指摘を踏まえ修正いたします。	「http://+++.****.jp/-----/(乙の用意するWeb上のページ)」	「https://+++.****.jp/-----/(乙の用意するWeb上のページ)」
221	一般社団法人 日本画像医療システム工業会	団体	03別紙1	68	6.5	“~メール若しくは書面により~”の“若しくは”は、“又は”にすべき。JISZ8301等参照。	ご指摘を踏まえ修正いたします。	「メール若しくは書面により」	「メール又は書面により」
222	一般社団法人 日本画像医療システム工業会	団体	03別紙1	68	6.5	“~書面若しくは暗号化が施された電子メール~”の“若しくは”は、“又は”にすべき。JISZ8301等参照。 同様に同ページ内の“メール若しくは書面”、“書面若しくは暗号化を施した電子メール“も修正。	ご指摘を踏まえ修正いたします。	「書面若しくは暗号化が施された電子メール」	「書面又は暗号化が施された電子メール」
223	一般社団法人 日本画像医療システム工業会	団体	03別紙1	70	6.5	“メール若しくはサービス利用画面等で行うことが望ましい”と記載されているが、 (1) 緊急対応なので、必要に応じて電話も併用すべきでは。 (2) “若しくは“は、”又は“にすべき (3) どれか1つの方法だけでなく、複数もありえるので“及び/又は”でつなぐ。 (変更案) ~電話、メール、及び/又はサービス利用画面等で行うことが望ましい	ご指摘を踏まえ修正いたします。	「メール若しくはサービス利用画面等で行うことが望ましい」	「電話、メール、サービス利用画面等で行うことが望ましい」
224	一般社団法人 日本画像医療システム工業会	団体	03別紙1	70	6.5	本項を定める上での考え方で、“ウ)事前承認及び事後承認“と記載しているが、上記の記載では、事後は報告であり、承認を記載していない。 (変更案) ウ)事前承認及び事後報告	ご指摘を踏まえ修正いたします。	「ウ)事前承認及び事後承認」	「ウ)事前承認及び事後報告」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
225	一般社団法人 日本画像医療システム工業会	団体	03別紙1	73	Ⅱ.6.6	P75の②サポート対応時間は、(1)利用者に対するサポートの下位の項になっている。このため、②のサポート時間は、利用者に対するサポート時間だと考える。本項を定める上での考え方では、(2)⑭を参照している。(2)⑭のタイトルは、“医療機関等の管理者からの問い合わせ窓口”となっており、利用者に対する窓口とは異なるように思える。医療機関等の管理者サポート、利用者のサポートを混乱しないように記載を修正すべき。	ここではシステムを利用する医師や医療機関等の管理者の両方が同じ窓口である場合を想定（事業者によっては別の場合もあるかと思います）しております。		
226	一般社団法人 日本画像医療システム工業会	団体	03別紙1	74	6.6	“本サービスの利用環境及びその設定に**関する確認**（OSやWebブラウザ、本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等及**び**乙が管理しないパソコンの機器の使用方法等に関する内容は含まない）”と記載されているが、()の前の確認の内容が()で記載されていると、()内が及びの前までが含む、及びの後ろが“”含まない”とも読めてしまう。誤解しないように明確に記載すべき。 下記、変更案1が趣旨だと思われる。 （変更案1）()内のOS、Webブラウザは含み、それ以降が全て含まない場合 本サービスの利用環境及びその設定に**関する確認**（OS、Webブラウザ等。ただし、以下は含まない。本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等、乙が管理しないパソコンの機器の使用方法等に関する内容） （変更案2）()内が全て含まない場合 本サービスの利用環境及びその設定に**関する確認**（ただし、以下は含まない。OS、Webブラウザ、及び本サービスで提供するアプリケーション以外のアプリケーション等、の使用方法等、並びに、乙が管理しないパソコンの機器の使用方法等に関する内容） （変更案3）()内の“及び”の前まで含み、“及び”の後が含まない場合 本サービスの利用環境及びその設定に**関する確認**（OS、Webブラウザ、及び本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等。ただし、以下は含まない。乙が管理しないパソコンの機器の使用方法等に関する内容）	ご指摘を踏まえ修正いたします。	「本サービスの利用環境及びその設定に関する確認（OSやWebブラウザ、本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等及び乙が管理しないパソコンの機器の使用方法等に関する内容は含まない）」	「本サービスの利用環境及びその設定に関する確認（OS、Webブラウザ等。ただし、以下は含まない。本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等、乙が管理しないパソコンの機器の使用方法等に関する内容）」
227	一般社団法人 日本画像医療システム工業会	団体	03別紙1	76	6.6	“規程ぶりを採用している”の”規程ぶり“はもう少しわかりやすい表現にすべき。 法律関係者が慣例として使っている“規定ぶり”とも少し違ったニュアンスで使っているようにも読める。 （変更前） 本SLAでは、対象事業者が講じるべき安全管理対策のうち、技術的な対応については、個別の対応措置の内容や方式、仕様等を明記せず、各項目において3．5に示す法令・ガイドラインの該当箇所を満たす対応を実施する、という**規程振りを採用**している。 （変更案） 本SLAでは、対象事業者が講じるべき安全管理対策のうち、技術的な対応については、個別の対応措置の内容や方式、仕様等を明記せず、各項目において3．5に示す法令・ガイドラインの該当箇所を満たす対応を実施する、という**ような記載**にしている。	ご指摘を踏まえ修正いたします。	「～規程振りを採用している。」	「～ような記載にしている。」
228	一般社団法人 日本画像医療システム工業会	団体	03別紙1	76	6.6	“変更都度資料提供を求める形”と記載しているが漢字が続き読みづらい。助詞を補い読みやすくすべき。 （変更案 ） 変更**の**都度**に**資料**の**提供を求める形	ご指摘を踏まえ修正いたします。	「変更都度資料提供を求める形」	「変更の都度に資料の提供を求める形」
229	一般社団法人 日本画像医療システム工業会	団体	03別紙1	77	6.6	“という規程振りをしている。” の”規程振り“はもう少しわかりやすい表現で記載すべき。 （変更案） という記載方法としている。	ご指摘を踏まえ修正いたします。	「～規程振りを採用している。」	「～ような記載にしている。」
230	一般社団法人 日本画像医療システム工業会	団体	03別紙1	78	Ⅱ.7.1	SLAの評価方法等が記載されているが、サービス稼働率が未達成の場合に未達成件数をどのように評価するか？1件？とするか？等明確に記載されていない。また、パターンファイル等は何をどのように数えて1件とするのか記載内容だけでは理解できない。	サービスレベルの評価方法については、あくまで事例であり、どのような指標を採用するかについては、対象事業者の提供するサービス内容や、SLAの内容等によって異なってくると考えております。		コメント案を記入いただければ。SLAの注記を転記
231	一般社団法人 日本画像医療システム工業会	団体	03別紙1	78	7.1	“ウイルス対策のためのパターンファイル**及び**OS**及び**ミドルウェア等のセキュリティパッチ”と記載されている。階層の異なる並列表記に両方とも“及び”が使われている。法律文章、あるいはJIS規格票（JISZ8301）に合わせて、及び、並びにを適切に使用すべき。 （変更案） ウイルス対策のためのパターンファイル**並びに**、OS**及び**ミドルウェア等のセキュリティパッチ	ご指摘を踏まえ修正いたします。	「ウイルス対策のためのパターンファイル及びOS及びミドルウェア等のセキュリティパッチ」	「ウイルス対策のためのパターンファイル並びに、OS及びミドルウェア等のセキュリティパッチ」
232	一般社団法人 日本画像医療システム工業会	団体	03別紙1	78	7.1	“ウイルス対策等の実施状況及び**の**実施率を管理指標”と記されているが、“及び“の後に”の“が変である。”の”の前に適切な名詞を補うか、この“の”を削除するかすべき。	ご指摘を踏まえ修正いたします。	「ウイルス対策等の実施状況及びの実施率を管理指標」	「ウイルス対策等の実施状況及び実施率を管理指標」
233	一般社団法人 日本画像医療システム工業会	団体	03別紙1	79	7.1	“ウイルス対策のためのパターンファイル及びOS及びミドルウェア等のセキュリティパッチ”と記載されている。階層の異なる並列表記に両方とも“及び”が使われている。 （変更案） ウイルス対策のためのパターンファイル**並びに**、OS**及び**ミドルウェア等のセキュリティパッチ	ご指摘を踏まえ修正いたします。	「ウイルス対策のためのパターンファイル及びOS及びミドルウェア等のセキュリティパッチの対応状況」	「ウイルス対策のためのパターンファイル並びに、OS及びミドルウェア等のセキュリティパッチの対応状況」
234	一般社団法人 日本画像医療システム工業会	団体	03別紙1	79	7.1	“サービスの内容や性格等勘案して”とあるが”性格“が少し変。 （変更案） サービスの内容や**特質等を**勘案して	ご指摘を踏まえ修正いたします。	「サービスの内容や性格等勘案して」	「サービスの内容や特質等を勘案して」
235	一般社団法人 日本画像医療システム工業会	団体	03別紙1	80	7.1	“対象事業者、医療機関等の両当事者**に**責め**に**帰すべからざる事由“と記載あるが、少し日本語が不自然。 （変更案） “対象事業者、医療機関等の両当事者**の**責め**に**帰すべからざる事由“	ご指摘を踏まえ修正いたします。	「対象事業者、医療機関等の両当事者に責めに帰すべからざる事由」	「対象事業者、医療機関等の両当事者の責めに帰すべからざる事由」
236	HEASNET事務局	団体	04別紙2	0	全般	対策項目の内容について、類似している内容が別の項目として定義してあるものが多数存在している。関係性を整理して項目自体の整理を行うべきではないか。	対策の類似性ではなく、「人的・組織的」・「物理的」・「技術的」の3つの対策の観点から整理しております。		
237	HEASNET事務局	団体	04別紙2	0	全般	関連する医療情報安全管理ガイドライン要求事項として、対策項目が紐づけられているが、医療情報安全管理ガイドラインの7章関連に関しては、e-文書法によって定義されている事項となるため、対象項目を除外する事業者が存在すると考えられる。基本的には6章の項目に紐づけた後に、e-文書法に対応するため追加で対策を行う項目に紐づけを行うべきではないか。	別紙2はリスクマネジメントの実践において事業者が確認する内容をまとめたもので、e-文書法等、関連する制度上の要求事項は別紙2にはまとめず、ガイドライン本体6章に記載しています。		
238	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	本書を参考に対策等を実施する必要があるが、本書の主体が、提供事業者である。医療情報安全管理ガイドラインは、主体が医療機関等である。これが混乱しないように記載する必要がある。例えば1.1②において、提供事業者は、持ち出した機器等に関して自身の運用管理規程に含め、医療機関等は、自身の運用管理規程に含める。さらに、医療機関等は、提供事業者の持ち出しが管理されていることを管理しないといけない。逆に提供事業者は、医療機関等が管理できるように支援しないといけない。この観点での記載が全般的に不足しているように感じる。 本書の対象する提供事業者は、さまざまか形態が示されている。例えば、1.1②に”持ち出し”に関して記載されているが、提供事業者が提供するサービス・システムが、医療機関等に設置される場合もある。クラウドなどの提供事業者の場合は、提供事業者の管理される場所に存在する。このあたりがかき分けられていないで、あたかも“クラウド”、“医療機関等の外部”のサービス、システムだけが対象の記載が散見される。 別紙2の1ページ目の表の解説で、対策項目が、”提供事業者が”主体的に実施する項目、“関連する医療情報安全管理ガイドライン”が医療機関等が主体的に実施する項目で提供事業者はそれを支援すべき項目であることを明記したほうがいいのではと思う。	ご指摘を踏まえ、一部記述を修正させていただきます。	「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方 ・対策項目 （追記） ・関連する医療情報安全管理ガイドラインの要求事項 （追記）	「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方 ・対策項目 「主な実施主体として、対象事業者を想定する。」 ・関連する医療情報安全管理ガイドラインの要求事項 「主な実施主体として、医療機関等を想定する。」
239	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	表の”推奨”の項目の説明として、“従前の情報処理事業者ガイドラインで「推奨される事項」に該当する項目”と記載されている。表の記載は“○”、“－”である。ここで、“－”が何を示すのかが読者にはわかりにくいのではないか。推奨でないことは理解できても、推奨より、より厳格に実施すべきなのかあるいは逆なのかがわかりにくい。特に表記で“－”だと、推奨より重要でないようにも見える。 また、従前のガイドラインでの表記だが、現時点で、本ガイドライン策定時の環境等を踏まえ、”推奨”のままなのかを有識者等の知見を元に記載すべきではないか。場合によっては、必要性が増した項目、あるいは逆な項目もあるのではないか。	記号を見直すとともに、対応表の見方に解説を追記いたします。	「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方 ・推奨 従前の情報処理事業者ガイドラインで「推奨される事項」に該当する項目	「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方 （削除） ・区分 ◎：従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインにおける遵守事項に該当 ○：従前の情報処理事業者ガイドラインにおける推奨事項に該当

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
240	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	“旧ガイドライン”の対策一覧を示し、本ガイドラインが旧ガイドラインと同等以上であると示す意図は理解できるが、最低限、現時点での状況に合わせた修正をすべき。	別紙2は、今般の2省ガイドラインの統合に際して、旧ガイドラインの対策項目を一覧化することに重点を置いており、可能な範囲での時点更新を行っているものであることにご理解ください。		
241	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	対象事業者が実施すべき対策項目とそれに関連する医療機関等が主体的に実施すべき医療情報安全管理ガイドラインを並べて記載されていて、非常にわかりやすく、参考になるのではと考える。しかし、医療情報安全管理ガイドラインのC項、D項全てが参照されているわけでない。記載のない医療情報安全管理ガイドラインのC項、D項に対して、対象事業者がそれらに関して全く関与する必要がないならば問題ない。しかし、まったく関与しないとは考えにくい。別紙に記載のない医療情報安全管理ガイドラインのC項、D項を抜き出してみた。これらに対する対象事業者の対策項目を記載して、表に追加すべきではないか。従来の経済産業省のガイドライン、総務省のガイドラインの抜けであるか、あるいは今回のスコープ変更に伴い必要なものかもしれない。	別紙2は、今般の2省ガイドラインの統合に際して、旧ガイドラインの対策項目を一覧化することに重点を置いており、可能な範囲での時点更新を行っているものであることにご理解ください。		
242	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	本ガイドラインは、JIS(日本産業規格)や法律文書ではないので、それらの規約に従う必然性はない。しかし、JIS等の記載方法などは誤解を受けない、わかりやすくする等のため、過去、多くの方のご尽力により改善、維持されてきたものである。本ガイドラインで、それらの記載方法等からの差異で気になるのは、下記に参考にすべきJISZ8301:2019 規格票の様式及び作成方法の対応箇条とともに記す。 (1) ぶらさがり段落 22.3.3 ぶら下がり段落 (2) 及び、並びに、又は、若しくは H.3.2.4 “又は”及び“若しくは”の用い方 H.3.2.2 “及び”, “並びに”及び“かつ”の用い方 上記の記載方法で本ガイドライン等で問題のある記載箇所は、後記にリストアップした。	ご指摘を踏まえ、一部記述を修正させていただきます。		（一部記述を修正）
243	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	対策項目の内容について、類似している内容が別の項目として定義してあるものが多数存在している。関係性を整理して項目自体の整理を行うべきではないか。	対策の類似性ではなく、「人的・組織的」・「物理的」・「技術的」の3つの対策の観点から整理しております。		
244	一般社団法人 日本画像医療システム工業会	団体	04別紙2	0	全般	関連する医療情報安全管理ガイドライン要求事項として、対策項目が紐づけられているが、医療情報安全管理ガイドラインの7章関連に関しては、e-文書法によって定義されている事項となるため、対象項目を除外する事業者が存在すると考えられる。基本的には6章の項目に紐づけた後に、e-文書法に対応するため追加で対策を行う項目に紐づけを行うべきではないか。	別紙2はリスクマネジメントの実践において事業者が確認する内容をまとめたもので、e-文書法等、関連する制度上の要求事項は別紙2にはまとめず、ガイドライン本体6章に記載しています。		
245	個人	個人	04別紙2	0	全般	「旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応」を「リスク対応確認項目表（旧両省ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応）」とする。	原案にても特段理解に支障がなく、原案のとおりとさせていただきます。		
246	一般社団法人 日本画像医療システム工業会	団体	04別紙2	3	1.1	“持ち出した機器に格納された情報が漏えいする**もしくは**、持ち帰った機器から不正なプログラムが感染拡大する。“とあるが、ここで、”もしくは”は、”又は“にすべき。(JISZ8301等参照。orは1つの場合は又は、階層になっている場合は、一番下の階層で”若しくは“を使う)	ご指摘を踏まえ修正いたします。	「持ち出した機器に格納された情報が漏えいするもしくは、持ち帰った機器から不正なプログラムが感染拡大する。」	「持ち出した機器に格納された情報が漏えいする又は、持ち帰った機器から不正なプログラムが感染拡大する。」
247	一般社団法人 日本画像医療システム工業会	団体	04別紙2	4	1.1	“サービスに“、”サービスに関する“、”サービスに供する“等の記載があるが、特定しなくても、本書の文脈で読めば明確ではないか。かえって特定してしまうことによって、本書の提供事業者の範囲にある、システムを提供する事業者に関する部分が除かれてしまうように読めてしまう。 このため、“サービスに“、”サービスに関する“、”サービスに供する“等の記載の削除。 他にも同様の記載があるので、同様に修正すべき。	ご指摘を踏まえ修正いたします。	1.1. 規程・手順の策定 ⑥-2 「サービスに供する機器及びソフトウェアの品質管理に関 する対応、手順等を運用管理規程等に含める。」	1.1. 規程・手順の策定 ⑥-2 「機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。」
248	一般社団法人 日本画像医療システム工業会	団体	04別紙2	5	1.1	保守作業は基本は事前承認だが、契約等により合意することにより承認が不要にすべき。これをしないと、パブリッククラウド事業者のサービスなどは運用できない。	ご指摘を踏まえ修正いたします。	「情報処理装置及びソフトウェアの適切な変更手順を策定する。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。」	「情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。」
249	一般社団法人 日本画像医療システム工業会	団体	04別紙2	5	1.1	“委託先に対して”とあるが、提供事業者から見ると委託先で間違いではないが、誤解をおこしにくい“再委託先に対して”に修正したほうがいい。	本ガイドラインは事業者の視点でまとめておりますので、原案の通りとさせていただきます。		
250	一般社団法人 日本画像医療システム工業会	団体	04別紙2	5	1.2	“個人情報の消去”とあるが、“個人を識別できる情報等の削除”のほうがより適切で、誤解を受けにくいのではないか。	ご指摘を踏まえ修正いたします。	「個人情報の消去」	「個人を識別できる情報等の削除」
251	HEASNET事務局	団体	04別紙2	7	1.5①-4	”C.最低限のガイドライン”ではなく、”D.推奨されるガイドライン”ではないか。	ご指摘を踏まえ修正いたします。	「C.最低限のガイドライン」	「D.推奨されるガイドライン」
252	一般社団法人 日本画像医療システム工業会	団体	04別紙2	7	1.5	区分に“C.最低限にガイドライン”と記載されているが、“D.推奨されるガイドライン”が正しい。	ご指摘を踏まえ修正いたします。	「C.最低限にガイドライン」	「D.推奨されるガイドライン」
253	一般社団法人 日本画像医療システム工業会	団体	04別紙2	7	1.5	“個人情報が物理的に保存されている機器や媒体は“とあるが、ここで、”物理的に”と言葉が少しわかりにくい。物理的だと紙に書かれているもののようなイメージになる。媒体には、電子的にかつその電子は物理的に記載されているので間違いではないがわかりにいくい。 また、文脈から、情報の参照ではなく、情報そのもののことを物理的にと表現しているようにも読めるがわかりにくい。“物理的に”を削除していいのでは。	ご指摘を踏まえ修正いたします。	「個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。」	「個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。」
254	一般社団法人 日本画像医療システム工業会	団体	04別紙2	10	1.9	“旧ガイドライン”の対策一覧を示し、本ガイドラインが旧ガイドラインと同等以上であると示す意図は理解できるが、最低限、現時点での状況に合わせた修正をすべき。 医療情報システムの安全管理に関するガイドラインが、旧版である4.1を参照している。最新版を適切に参照し、必要に応じて最新版に対応した記載にすべき。	ご指摘を踏まえ修正いたします。	医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 4.1 版」6.8 章 C 項の管理策を実施する。	「医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第5版」6.8 章 C 項の管理策を実施する。」
255	一般社団法人 日本画像医療システム工業会	団体	04別紙2	10	1.9	“受託事業者もしくは外部事業者”と記載しているが、”もしくは”ではなく、”又は“にすべき。	ご指摘を踏まえ修正いたします。	「受託事業者もしくは外部事業者」	「受託事業者又は外部事業者」
256	一般社団法人 日本画像医療システム工業会	団体	04別紙2	10	1.10	“過少もしくは“過剰となる”と記載しているが、”もしくは”ではなく、”又は“にすべき。	ご指摘を踏まえ修正いたします。	「過少もしくは費用対効果の観点で過剰となる。」	「過少又は費用対効果の観点で過剰となる。」
257	一般社団法人 日本画像医療システム工業会	団体	04別紙2	11	1.11	“実施できないことで、必要な講じられない。”は、日本語が変。必要な何？何を講じられない？関連する医療情報安全管理ガイドライン要求事項には、所管官庁への連絡まで記載がないので、変更案として下記。 ”ことで、必要な講じられない。“を削除し、“実施できない。”とすべき。	ご指摘を踏まえ修正いたします。	「サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な講じられない。」	「サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。」
258	一般社団法人 日本画像医療システム工業会	団体	04別紙2	13	1.13	本番環境と開発環境とが分離していることは重要あり、特に”システム”の場合は、“直接に接続”されていない状態が有効である。しかし、クラウド等の”サービス“の場合は、”直接に接続“は、少し無理があるのではないかと思われる。もしかしたら、クラウドの本番とは別の”テナント”を開発環境にするかもしれない。	ご指摘を踏まえ修正いたします。	「ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行う。」	「ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。」
259	一般社団法人 日本画像医療システム工業会	団体	04別紙2	14	1.14	関連する医療情報安全管理ガイドライン要求事項の内容に記載されている、“(2)見読化手段の管理”の”見”の上の四角に×マークの記号が重なってしまっている。	ご指摘を踏まえ修正いたします。		（文字を再度貼付）
260	一般社団法人 日本画像医療システム工業会	団体	04別紙2	14	1.14	①-1の3行だけで1Pageとなってしまっている。工夫して、Pageを有効に活用すべき。	ご指摘を踏まえ修正いたします。		（ページ設定見直し）
261	HEASNET事務局	団体	04別紙2	15	1.14②-4	②-3ではないか。	ご指摘を踏まえ修正いたします。	「②-4に定めた手順を医療機関等に示し」	「②-3に定めた手順を医療機関等に示し」
262	HEASNET事務局	団体	04別紙2	15	1.14②-5	②-3ではないか。	ご指摘を踏まえ修正いたします。	「②-5で示された手順について」	「②-3で示された手順について」
263	一般社団法人 日本画像医療システム工業会	団体	04別紙2	15	1.14	“②-4に定めた手順～”と記載されているが、“②-3”の誤り。	ご指摘を踏まえ修正いたします。	「②-4に定めた手順」	「②-3に定めた手順」
264	一般社団法人 日本画像医療システム工業会	団体	04別紙2	15	1.14	“②-5に定めた手順～”と記載されているが、“②-3”の誤り。	ご指摘を踏まえ修正いたします。	「②-4で示された手順」	「②-3で示された手順」
265	HEASNET事務局	団体	04別紙2	19	2.3①-1	”C.最低限のガイドライン”ではなく、”D.推奨されるガイドライン”ではないか。	ご指摘を踏まえ修正いたします。	「C.最低限のガイドライン」	「D.推奨されるガイドライン」
266	一般社団法人 日本画像医療システム工業会	団体	04別紙2	19	2.3	区分に“C.最低限にガイドライン”と記載されているが、医療情報安全管理ガイドラインでの記載は“D.推奨されるガイドライン”が正しい。もし、必須にするなら、区分以外の列(例えば、推奨)を用いて、必須する旨を記載できるようにしたほうがいい。	ご指摘を踏まえ修正いたします。	「C.最低限にガイドライン」	「D.推奨されるガイドライン」
267	一般社団法人 日本画像医療システム工業会	団体	04別紙2	19	2.4	“医療機関等に提供する**医療情報システム**の継続に必要であれば、受託する医療情報のバックアップ施設等、**情報処理医療情報システム**を継続するための～”と記載あるが、 ”情報処理医療情報システム”は言葉が変。元の経済産業省のガイドラインの“情報処理サービス”を”医療情報システム“に置き換えているようだが、2つ目は、置き換えが中途半端で、”情報処理“を消し忘れている。	ご指摘を踏まえ修正いたします。	「情報処理医療情報システムを継続するための代替情報処理施設を設置し」	「医療情報システムを継続するための代替情報処理施設を設置し」

No.	氏名・名称	属性	資料	ページ	パート	意見	方針・コメント	修正内容	
								原案	修正案
268	一般社団法人 日本画像医療システム工業会	団体	04別紙2	19	2.6	別途、実施されている厚労省の医療情報安全管理ガイドラインの改定においても、コメントされ採用されているが、“盗難防止用チェーン”は、”盗難防止用チェーン等”に修正。	ご指摘を踏まえ修正いたします。	「盗難防止用チェーンを取り付ける。」	「盗難防止用チェーン等を取り付ける。」
269	一般社団法人 日本画像医療システム工業会	団体	04別紙2	20	2.8	“地震、水害、落雷、火災等並びにそれにともなう停電等”とあるが、“並びに”の使い方が適切でない。“地震、水害、落雷、火災等、及び、それに伴う停電等”あるいは、“地震、水害、落雷、及び火災等、並びにそれに伴う停電等に”のどちらかにすべき。	ご指摘を踏まえ修正いたします。	「地震、水害、落雷、火災等並びにそれにともなう停電等」	「地震、水害、落雷、火災等、及び、それに伴う停電等」
270	一般社団法人 日本画像医療システム工業会	団体	04別紙2	22	3.1	“、”(読点)、“又は”の使い方が正しくなく、読みづらい。 (変更前) “ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号(PIN)、パスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせた多要素認証” (変更案) 1. “ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号(PIN)又はパスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせた多要素認証” 2. “ログオン時に利用する認証要素としては、ハードウェアトークン若しくは IC カード等の認証デバイス、暗証番号(PIN)若しくはパスワード等の記憶要素、又は、生体情報(バイオメトリクス)等を組み合わせた多要素認証”	ご指摘を踏まえ修正いたします。	「ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号(PIN)、パスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせた多要素認証」	「ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号(PIN)又はパスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせた多要素認証」
271	一般社団法人 日本画像医療システム工業会	団体	04別紙2	22	3.1	”利用者の認証において、固定式のID・パスワードによる認証方式を採用している場合には、固定式のID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。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年後を目途に多要素認証について厚生労働省ガイドライン6.5章「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。” この文書は、多要素認証の1要素とする場合は、”固定式のID・パスワード” を用いてよいと読み取れる。また、用いてよいのであれば、3.1. 利用者認証の実装　④安全なパスワード要件の定義　と矛盾する。 そもそも”固定式のID・パスワード”は、現在の3省3ガイドラインに記載のないものであり、⑤-4 の記載は不要でないか？	ご指摘を踏まえ修正いたします。	「利用者の認証において、固定式のID・パスワードによる認証方式を採用している場合には、固定式のID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。」	「利用者の認証において、ID・パスワードによる認証方式を採用している場合には、ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。」
272	一般社団法人 日本画像医療システム工業会	団体	04別紙2	23	3.3	“情報処理装置上”と記載しているが、他に合わせて“医療情報システム上”にすべき。	ご指摘を踏まえ修正いたします。	「利用者は情報処理装置上においてユニークな利用者ごとのID により識別する。」	「利用者は医療情報システム上においてユニークな利用者ごとのID により識別する。」
273	一般社団法人 日本画像医療システム工業会	団体	04別紙2	24	3.3	特権IDが不正利用もしくは乗っ取られることにより”の”もしくは”は、”又は“にすべき。	ご指摘を踏まえ修正いたします。	「特権IDが不正利用もしくは乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。」	「特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。」
274	一般社団法人 日本画像医療システム工業会	団体	04別紙2	25	3.3	“情報処理装置”と記載しているが、他に合わせて“医療情報システム”にすべき。	ご指摘を踏まえ修正いたします。	「情報処理装置及びソフトウェアを使用する前に」	「医療情報システム及びソフトウェアを使用する前に」
275	一般社団法人 日本画像医療システム工業会	団体	04別紙2	26	3.4	安全管理ガイドラインの“内容”において、6.8D5の内容が記載されているが、最後に余分な6.8D4の文章の切れ端が記載されてしまっている。 “ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。”	ご指摘を踏まえ修正いたします。	「5. 保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。」	「5.保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。」
276	HEASNET事務局	団体	04別紙2	28	3.7①	”6.5 技術的安全対策”ではなく、”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”ではないか。	ご指摘を踏まえ修正いたします。	「6.5 技術的対策」	「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」
277	一般社団法人 日本画像医療システム工業会	団体	04別紙2	28	3.6	②端末やサーバの堅牢化とあるが、①の間違い。	ご指摘を踏まえ修正いたします。	「②端末やサーバの堅牢化」	「①端末やサーバの堅牢化」
278	一般社団法人 日本画像医療システム工業会	団体	04別紙2	28	3.7	安全管理ガイドラインの“項番”と“内容”とが対応していない。 項番が6.5 技術的対策と記載されているが、6.11外部と診療情報等を含む医療情報を交換する場合の安全管理の記載間違いではと思われます。	ご指摘を踏まえ修正いたします。	「6.5 技術的対策」	「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」
279	一般社団法人 日本画像医療システム工業会	団体	04別紙2	31	3.8	安全管理ガイドラインの“内容”の記載で、安全管理ガイドラインの本文と合わせて、“12.無線LANを利用する場合”の後で改行をいれるべき。	ご指摘を踏まえ修正いたします。	「12.無線 LAN を利用する場合システム管理者は以下の事項に留意すること。」	「12.無線 LAN を利用する場合 システム管理者は以下の事項に留意すること。」
280	一般社団法人 日本画像医療システム工業会	団体	04別紙2	33	3.11	関連する医療情報安全管理ガイドライン要求事項の内容に記載されている、“4.スマートフォン~”の”ス”の上の四角に×マークの記号が重なってしまっている。	ご指摘を踏まえ修正いたします。		(文字を再度貼付)
281	一般社団法人 日本画像医療システム工業会	団体	04別紙2	33	3.13	“IPSec”の”S”は小文字の表記にすべき。つまりIPsec	ご指摘を踏まえ修正いたします。	「IPSec」	「IPsec」
282	一般社団法人 日本画像医療システム工業会	団体	04別紙2	36	3.18	関連する医療情報安全管理ガイドライン要求事項の内容に記載されている、”③見読目的に応じた応答時間” の”見”の上の四角に×マークの記号が重なってしまっている。	ご指摘を踏まえ修正いたします。		(文字を再度貼付)
283	一般社団法人 日本画像医療システム工業会	団体	04別紙2	37	3.20	“PNG等のフォーマット46)”と記載されているが、“46”は不要。元の経産省の要求事項の文章についていた脚注の番号。脚注46には 46 Portable Document Format、Joint Photographic Experts Group、Portable Network Graphicsと、各フォーマットの正式英語が記載されているだけなので、不要。	ご指摘を踏まえ修正いたします。	「PDF、JPEG 及び PNG 等のフォーマット46)」	「PDF、JPEG 及び PNG 等のフォーマット」
284	一般社団法人 日本画像医療システム工業会	団体	04別紙2	37	3.20	“障害等が生じた場合**のを**明確にした上で”と記載されているが日本語が変。 (修正案) “障害等が生じた場合**の責任分界を**明確にした上で“	ご指摘を踏まえ修正いたします。	「障害等が生じた場合のを明確にした上で」	「障害等が生じた場合の役割分担を明確にした上で」
285	一般社団法人 日本画像医療システム工業会	団体	04別紙2	37	3.21	“~③の運用管理規程に定める~”と記載されているが”③”は”①-4”の間違い	ご指摘を踏まえ修正いたします。	「③の運用管理規程に定める管理方法への対応等を求める」	「①-4の運用管理規程に定める管理方法への対応等を求める」
286	グーグル・クラウド・ジャパン合同会社	団体	04別紙2	71	1.5.③-1	当該内部監査の削除、若しくは国際(ISO,SOCなど)・国内(JISやプライバシーマークなど)基準の資格取得により、内部監査と同様とみなす旨にご修正頂く様お願いしたく存じます。	内部監査の実施と国際・国内基準の資格取得はその目的等が異なると考えられ、原案のとおりとさせていただきます。		