「医療情報システムの安全管理に関するガイドライン第6.0版（案）」に関する御意見募集の結果について

（別紙）

No.	分類	編	章	頁	御意見	回答（考え方）
1	全体構成の見直し	すべて	―	―	全資料読む必要がある人向けの各編合冊版の刊行予定はあるか。	現時点において、合冊版の刊行予定はございません。
2	全体構成の見直し	すべて	―	―	大幅な文書構造の変更、4つの編の新規作成、付属する多数の文書群の作成、整備等とともに、医療機関でのランサムをはじめ多数の事件、事故に対する対応等、作成された方々に敬意を表します。	御意見ありがとうございます。
3	全体構成の見直し	すべて	―	―	C項、D項がなくなったことにより総務省/経済産業省の「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」の別紙2の対応表が大きく影響を受ける。総務省、経済産業省に適切に変更内容を効果的に伝えて欲しい。	御意見として参考にさせていただきます。
4	全体構成の見直し	システム運用編（Control）	３．責任分界	P5	【遵守事項】の中で、担当者に対応を指示しているものが、システム運用編の【遵守事項】で指示に基づいた記述になっていない箇所がある。対応づけられるものに関しては遵守事項として「企画管理者の指示の下」という対応づけを行った方がいいのではないか。 （案）②事業者 と技術的な対応に関する責任分界を調整する際に、 企画管理者の指示の下、要求仕様と の適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。	御意見として参考にさせていただきます。
5	全体構成の見直し	概説編（Overview）	３．２．２ 医療機関等の特性に応じたガイドライン参照箇所	P4	パターンI又はIIにおいてシステム運用管理者がどれを読むのか、企画管理者がどれを読むのかも明記しておくべきでは。	表３－２において、企画管理者及びシステム運用管理者が参照すべき項目について示しています。
6	全体構成の見直し	概説編（Overview）	３．２．２ 医療機関等の特性に応じたガイドライン参照箇所	P4	パターンIとIII又はIIとIVとは前記の置き換え以外同じ記載になっている。もう少し表の記載方法、体裁を考慮してわかりやすくすべきではないか。	御意見として参考にさせていただきます。
7	全体構成の見直し	概説編（Overview）	３．２．２ 医療機関等の特性に応じたガイドライン参照箇所	P5	概説編の表3-1,表3-2の前に「システム運用専任の担当者」、「システム運用管理者」又は「企画管理者」の用語の説明、関係を明記したほうがいいのでは。	「企画管理者」と「システム運用管理者」という文言が混在していたため、「企画管理者」に統一いたしました。また、企画管理者またはシステム運用担当者の定義については、企画管理編またはシステム運用編の【はじめに】で示しています。
8	全体構成の見直し	経営管理編（Governance）	―	―	「管理」の言葉が企画管理編ともダブっているため「医療経営編」などでどうでしょうか。	御意見として参考にさせていただきます。
9	全体構成の見直し	すべて	―	―	「遵守事項」の位置付けが不明確であり（第5.2版の「C」項？）、ベースライン型をリスクベース型にする時の典型的混乱が表れていると思われ、この位置づけを明記しないと、ユーザに不要な混乱を生じさせる恐れがあると思います。	御意見として参考にさせていただきます。
10	全体構成の見直し	すべて	―	―	第5.2 版「3.4　取扱いに注意を要する文書」の内容は、「総務・経産2 省ガイドライン “6.4 取扱いに注意を要する文書等の要求事項 “にそのまま転記があること等から、適切な場所に等価な記載内容を示してほしい。	ご指摘の記載については、Q&A（概Q-3）に記載してあります。
11	全体構成の見直し	すべて	―	―	現時点の安全管理ガイドラインを実施している医療機関等にとっては、変更箇所が非常にわかりにくくなってしまったように感じる。 遵守事項を外部文書から参照する機会が多くなるが、4編全ての遵守事項にユニークな参照記号番号等があるといいのではないか。	第5.2版との関係については、第5.2版→第6.0版項目移行対表を参照してください。
12	全体構成の見直し	概説編（Overview）	３．１ 各編の目的・概要	P3	企Q-17、-25、-26等、Q&Aの多くの内容が必読の内容であるため、読み落としが無いように「3.1　各編の目的・概要」箇所で、Q&Aについて言及して欲しい。	御意見として参考にさせていただきます。
13	全体構成の見直し	他(参考資料)	―	―	第5.2版まで存在した付表1、２、３が廃止されたのであれば「不要とした判断の説明」が欲しい。	本ガイドラインは、5.2版の付表の代わりに、専任のシステム担当者の有無や導入している医療情報システムの形態の違いに応じてガイドラインの参照パターンを分類してお示ししています。
14	全体構成の見直し	すべて	―	―	5版より大きく構成も変わり役割分担が明確になったが、病院内において企画管理者像をもった人材は内部では存在しないと思われる。そのため経営管理でもとめられるものはこの企画管理者を雇う、もしくは外部委託するなどしっかりできる管理者を任命することが必要であるのでそういったガイドライン記載が欲しい。また病院内ではセキュリティの運用担当者など通常存在しないため、診療情報管理士のように診療報酬上での作業の範囲の明確さや人員の配備などを明確に行ってほしい。	御意見として参考にさせていただきます。
15	全体構成の見直し	概説編（Overview）	３．本ガイドラインの構成、読み方	P2	図３－１は３つの編が独立しているように見え、経営者編の要求に対する具体施策が企画管理及びシステム運用編でどのように展開されて記載されているか等理解できないと思われることから、「参考７」各編相関表のサマリを図３-１の後に付けてはどうか。	御意見として参考にさせていただきます。
16	全体構成の見直し	経営管理編（Governance）	【はじめに】 ＜経営管理編の構成と概要＞	P2	指示を出す経営者もガイドライン全体の構成を理解した方が良いと思われ、５つの章の具体的な施策が企画管理編及びシステム運用編に書かれていることを明記してはどうか。	御意見として参考にさせていただきます。
17	全体構成の見直し	システム運用編（Control）	【はじめに】 ＜医療機関等の 特性に応じたガイドライン参照箇所＞	P1	「医療機関等の特性に応じた本ガイドラインの参照パターン」という表において、本書の内容から、オンプレミスとクラウドに分ける必要がなく、また、3・4において、「担当者」を「システム管理者」に置換となっており表現を変える必要がないことから、区分けとしては1・3、2・4のみが妥当と考える。	御意見として参考にさせていただきます。

18	全体構成の見直し	すべて	―	―	本改定の趣旨は、「医療情報システムの安全管理の実効性を高める観点から各編で想定する読者に求められる遵守事項やその考え方を示すとともに、Q&A等で現状選択可能な具体的技術に言及する」形に改変することにあると理解しましたし、その趣旨には強く賛同します。	御意見ありがとうございます。
19	全体構成の見直し	―	―	―	概説編の表３－１の横軸は医療情報システムが「オンプレミス」であるか「クラウド」であるかではなく、システムを自ら導入して運用しているか、外部のサービスを利用しているかを示していると考えられ、縦軸はシステム運用を自組織の担当者が担っているか、外注・委託しているシステム運用管理者が担うかを示していると考えられ、さらに概説編の表３－２では、担当者の有無の差は「※ 各編内の「担当者」という記載を「システム運用管理者」に置換し、参照。」という言葉のみであり本質的な違いは無いと考えられることから、 ①表３－１の「オンプレミス型」「クラウドサービス型」の表現は「システム導入型」「サービス利用型」という表現に変更してはどうか。 ②表３－１のなお書きは、院外のサービスに医療情報を預けて居る場合についての記載でであるため参照パターンはIIIやIVではなく、IIやIVが適切ではないか。 ③表３－１の縦軸は廃し、「システム運用担当者は、医療機関等に専任で置かれた医療情報システムを直接操作する者、もしくは、医療情報システムの運用の委託・外注をうけた者（の責任者）を意味する」ことを、用語の定義等に明記し、関連項目を整理してはどうか。 ④企画管理編２．２．２（２）の３パラの「SaaSの利用」は、表３－１の右半分の事例（サービス利用型）に該当する場合であると考えられることから、文全体の整合性を維持するため、事例を、PaaSやIaaSに改め、責任分界の一部が医療機関にある場合に変更してはどうか。	②についてはご指摘を踏まえ修正いたします。①、③、④については、今後の検討にあたっての参考とさせていただきます。
20	全体構成の見直し	概説編 （Overview）	３．３ 第 5.2 版との関係	P6	Ｑ＆Ａはあくまで補足とし、必要な事項は各編で記述してほしい。	ご指摘の通り、本文について、経営管理編、企画管理編、システム運用編に分け、それぞれに求められる遵守事項やその考え方を示すとともに、Q&A（企Q-54）では現状可能な具体的技術にも言及しています。
21	全体構成の見直し	企画管理編 （Management）	―	P9 P10 P13 P20	以下について、第5.2版の付表にあった「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」のような作成例を作成いただき、求められる基準、規定等の作成にあたり必要事項が漏れないようにして欲しい。 ・１．２．１ 情報セキュリティ方針（ポリシー）等の策定 ・２．１．１ 医療機関等における責任と責任分界 ・２．２．２ 委託における責任分界（複数事業者が関与する場合を含む） ・４．２ 規程の整備（運用管理規程ほか）	本ガイドラインは、5.2版の付表の代わりに、専任のシステム担当者の有無や導入している医療情報システムの形態の違いに応じてガイドラインの参照パターンを分類してお示ししています。
22	全体構成の見直し	概説編 （Overview）	３．１ 各編の目的・概要	P3	「特集：小規模医療機関等向けガイダンス」を有効に活用してもらうために、概Ｑ－９の記載内容を基に本編本項にて３．１．５として以下追記をしてはどうか。 （追記案） ３．１．５　小規模医療機関等向けガイダンス 医療機関等においては、専任の情報システム運用担当がいない場合や、医療情報システムを外部のクラウドサービスにするなどで、医療機関等の直接的な負担を軽減し、安全な医療情報の取り扱いを図るため、外部の医療情報システム・サービス事業者に運用等を委ねる場合があり、小規模医療機関等において、特にみられる傾向と言えます。第６．０版では、このように医療機関等の規模の大小ではなく、医療機関等における体制や、医療情報システムの構成に着目し、医療機関等に専任のシステム運用担当者が存在しない場合や、利用する医療情報システムがクラウドサービスだけの場合には、本ガイドラインの一部については、参照を簡略化できることとしています。 このように小規模医療機関等における対策の負担軽減を直接示す内容は含まれていないものの、実質的には外部委託の活用等の対応が図れるようにしています。また、診療所や薬局等の小規模医療機関等向けの特集も、補足資料として用意していますので、適宜、ご参照ください。	御意見として参考にさせていただきます。
23	新技術、制度・規格の変更への対応	システム運用編 （Control）	５．システム設計の見直し（標準化対応、新規技術導入のための評価等）	P12	「① システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。」は、現在、当該機能を備える電子カルテシステムは市販されていないことから実効性が確保されないことが想定され、以下修正を要望する。 「① システム更新の際は、爾後のシステム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。」	御意見として参考にさせていただきます。
24	新技術、制度・規格の変更への対応	システム運用編 （Control）	１３．ネットワークに関する安全管理措置	P34	【遵守事項】⑥は、１．TLS全体の機能（暗号化や認証技術の集合体）とTLSクライアント認証が混同されている点、及び２．TLSクライアント認証に技術が限定されている点から修正を希望します。TLSクライアント認証は、証明書をインストールしたクライアント（端末）をサーバー側で認証する技術であり、適切な端末からのアクセスを担保するだけのもので、TLSクライアント認証に期待する効果は、サーバー側が悪意の第三者をはじく効果と認証された端末以外からのアクセスを防ぐ効果の両面と思われますが、前者については同編14.利用者認証にて確保されること、また後者についてはMDM等により端末管理を適切に行うことで代替できることから、TLSクライアント認証に手段を限定する必要性はないものと認識。以上を踏まえ、例えば、該当箇所一文目については単に「オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLS のプロトコルバージョンをTLS1.3 以上に限定すること。」とした上で、項目の末尾に「なお、接続先となる端末の真正性担保のため、TLSクライアント認証による端末の認証や適切な端末管理を行うとともに、14に記載の利用者認証を行うこと。」を追記するといった修正をすべき。	今後の検討事項とさせていただきます。
25	新技術、制度・規格の変更への対応	企画管理編 （Management）	３．安全管理のための体制と責任・権限	P17	【遵守事項】⑨の記載は、３．１．８項では「必要な体制を整備することが求められる。」とあることから、下記の通りに修正してはどうか。 （変更案）9 患者等からの・・・の体制を整備すること。	御意見として参考にさせていただきます。

26	新技術、制度・規格の変更への対応	企画管理編（Management）	１４．法令で定められた記名・押印のための電子署名	P50	【遵守事項】は記述が煩雑で要求内容が読み取れず整理してもらいたい。	御意見として参考にさせていただきます。
27	新技術、制度・規格の変更への対応	システム運用編（Control）	１８．外部からの攻撃に対する安全管理措置	P48	【遵守事項】①の「バックアップからの重要なファイルの復元」のあとに付く（）文は解説文で説明しているので不要ではないか。	御意見として参考にさせていただきます。
28	新技術、制度・規格の変更への対応	システム運用編（Control）	１１．システム運用管理（通常時・非常時等）	P28	【遵守事項】は非常時に対する独立した要求で良いと思われ、「非常時の医療情報システムの運用について、次に掲げる対策を実施すること。」とした中で①～⑦としてはどうか。 （変更案） 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。 ①「非常時のユーザアカウントや非常時用機能」の手順を整備すること。 ②　非常時機能が 通常 時に不適切に利用されることがないようにするとともに、・・・。 ③　非常時用ユーザアカウントが使用された場合、・・・。 ④　医療情報システムに不正ソフトウェアが混入した場合に備えて、・・・。 ⑤　サイバー攻撃による被害拡大の防止の観点から、・・・。 ⑥　重要なファイルは数世代バックアップを複数の方式 で 確保 し、・・・。 ⑦　医療情報システムの稼働状況などを把握するため、・・・。	御意見として参考にさせていただきます。
29	新技術、制度・規格の変更への対応	企画管理編（Management）	１４．１ 法令で定められた記名・押印のための電子署名の要件	P53	「ISO14533-1：2014CMS利用電子署名(CAdES)の長期署名プロファイル」とあるが、ISO14533-1の最新版「ISO14533-1：2022」を参照するよう修正したほうが良いのではないか。	ご指摘踏まえ修正いたします。
30	新技術、制度・規格の変更への対応	システム運用編（Control）	１４．認証・認可に関する安全管理措置	P41	医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行うのに二要素認証を必須とすることを継続するのでしょうか。	二要素認証技術の端末等への実装については、医療機関等の負担を考慮し、令和9年時点で稼働していることが想定される医療システムを、今後導入または更新する場合に原則として求めることとしています。
31	新技術、制度・規格の変更への対応	システム運用編（Control）	１４．認証・認可に関する安全管理措置	P41	【遵守事項】⑤に「利用者認証にパスワードを用いる場合には、」とあるが、パスワードを使用しない場合もあるということでよいか。	IDとパスワード以外の手段として、ICカード、電子証明書、生体認証等を用いることも想定されます。
32	新技術、制度・規格の変更への対応	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	クライアント認証の目的は接続端末を固定することにあり、目的を達成するための手段はクライアント証明書以外にもありますので、手段を限定することは不適切であることから、【遵守事項】⑥は「クライアント証明書を利用したTLSクライアント認証等を実施することによりサービスに接続できる端末を制限すること。」と修正することを提案する。	今後の検討事項とさせていただきます。
33	新技術、制度・規格の変更への対応	システム運用編（Control）	７．情報管理（管理・持出し・破棄等）	P16	【遵守事項】⑬はVPN + 仮想デスクトップのみを推奨しているような記述に読め、現在VPN を利用せずに同等以上の安全性を確保できるゼロトラストという方法もあるため、特定技術を明示しない方が適切。	御指摘を踏まえ、VPNと組み合わせた仮想デスクトップに技術を限定しないような書きぶりに修正いたしました。
34	新技術、制度・規格の変更への対応	システム運用編（Control）	７．情報管理（管理・持出し・破棄等）	P16	【遵守事項】⑬において、利用者による外部からのアクセスを許可する場合は、システムの特性もあるため、「利用者による外部からのアクセスを許可する場合は、外部からアクセスする際に院内システムに不正アクセスされた場合の影響を減らすために、サーバー等へ直接アクセスさせるのではなく、例えば、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定するなどの対応が必要である。」としてはどうか。	御意見として参考にさせていただきます。
35	新技術、制度・規格の変更への対応	システム運用編（Control）	７．４ 医療情報を格納する記録媒体、情報機器等の紛失、盗難等が生じた場合の対応	P20	MDMでなく、状況環境により様々な方策（例：複数回のパスワード入力失敗で、自己自動消去機能等）が考えられることから、「例えば、」から始まる箇所は「例えばモバイル端末については、持ち出し端末の記録媒体の暗号化等の対策が求められる。また、MDM（Mobile Device Management ）を導入することで、遠隔制御を行うことも有効である。」等としてはどうか。	御意見として参考にさせていただきます。
36	情報セキュリティに関する考え方の整理	企画管理編（Management）	１５．技術的な安全管理対策の管理	P55	「② 個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定すること。」は、看護師詰書のような多くのスタッフが出入りする閉空間ではない場所に電子カルテ端末が設置されていたり、医師の働き方改革等で推奨されるであろうテレワーク環境における電子カルテ等の諸記録の閲覧等を鑑みると、入退室管理（施錠、識別、記録）を適切に行えないことが想定され、以下修正を要望する。 修正案：「② 個人情報データベースが保存されているサーバが設置された区画に対しては、入退室管理（（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定すること。個人情報の入力・参照可能な端末等が管理されている区画において、識別された端末操作者以外が情報を閲覧できないような措置（※）を講じること。医療機関等の施設外からの入力・参照等が可能な端末等についても識別された端末操作者以外が情報を閲覧できないような措置を講じること。」※：画面の視野角を制限するフィルムの画面貼付や一定時間経過時のスクリーンセーバー等。	ナースステーションにおける入退室管理についてはQ&Aに記載しています。また、外部端末からのアクセスについては、ご指摘の趣旨を踏まえ、「医療機関等の施設外からの入力・参照等が可能な端末等についても同様である」の文言は削除します。

37	情報セキュリティに関する考え方の整理	システム運用編（Control）	１４．認証・認可に関する安全管理措置	P41	「⑤ 利用者認証にパスワードを用いる場合には、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、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。」 「⑥ パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。 － 類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。 － 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。」 の、⑥の２点は、現在稼働している電子カルテシステムでは未対応のソフトウェアが広く使われていることから実効性が確保されないと思われ、以下修正を要望する。 「⑤ 利用者認証にパスワードを用いる場合には、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、新規導入又は更新に際しては、次に揚げる対策を実施すること。 － 二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。 － 類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。 － 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。」 「⑥ パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。」	御意見として参考にさせていただきます。
38	情報セキュリティに関する考え方の整理	概説編（Overview）	３．２．１ 医療機関等の特性についての考え方	P4	『本ガイドラインは、すべての医療機関等における医療情報システムを対象とした安全管理に関して、各編で遵守事項やその考え方等を示している』との記載は、従前のガイドラインにおける「C項」に該当する必要最低限実施すべき事項なのか、セキュリティ管理を行う上で遵守を目的とすべき管理要件であり、リスク評価の結果に基づき対応要否を主体的に検討すべきものという位置づけなのか、＜遵守事項＞の定義を明確にすべき。 あわせて今回のGLは、今までのベースラインアプローチ（to Doを列記し、「これだけやればよい」とする考え方）から、リスクベースアプローチ（病院個々のシステム固有要件に基づき、想定されるリスクを抽出し、実施すべき対策水準を検討する考え方）へ変化している点を概説編で明示的に説明することが必要ではないか。	遵守事項は、従前のガイドラインにおけるC項（最低限のガイドライン）及びD項（推奨されるガイドライン）を想定しています。リスクベースアプローチに関する記載へのご指摘は、今後の検討において参考にさせていただきます。
39	情報セキュリティに関する考え方の整理	経営管理編（Governance）	【はじめに】	P1	『安全管理対策の実施を「コスト」と捉えるのではなく、質の高い医療の提供に不可欠な「投資」と捉えることも重要である』との記載がある一方で、経営管理編のどこにも、セキュリティ投資予算・リソースについて経営層が確保すべきという記載が一切見られない。 「サイバーセキュリティ経営ガイドライン」では触れている予算・リソースの確保をマネジメント層が果たすべき責務として経営管理編で定義してはどうか。	ご指摘を踏まえ、経営管理編において、安全管理対策の実施に必要となる資源（予算・人材等）の確保に努めることが重要である旨を追記しました。
40	情報セキュリティに関する考え方の整理	経営管理編（Governance）	２．２．２ 情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の実践	P10	遵守事項に、ISMSを策定し実施することが定義されている点は、一般的な意味での情報セキュリティマネジメントプロセス（ISMS）を策定することが必要という意味であり、医療機関がISMSを取ること自体を目的とせぬよう、ISMS認証＝ISO27001を取得することが目的ではない点を明記すべき。	ご指摘を踏まえ、Q&A（企Q-27）において、プライバシーマークやISMS認証は医療情報を取り扱う医療情報システムサービス事業者として最低限取得すべきものである旨の考え方を追記いたします。
41	情報セキュリティに関する考え方の整理	企画管理編（Management）	９．２ 情報機器等の安全性の確認	P38	・「９．２情報機器等の安全性の確認」で『企画管理者は担当者に情報機器等の安全に関する情報の収集（利用している情報機器等やシステム、プログラム等）と、それを踏まえた対応を指示、その対応状況を確認すること）で、情報機器等の安全性を定期的に確認する必要がある』とあるが、病院のセキュリティ予算は著しく限定されている。そうしたなかで、企画管理者のリソースの限定性を考慮した場合、あくまでベンダーからの報告指示＆内容協議・相談こそが重要であるという立て付けにしない限り、絵にかいた餅にしかならない。200床以下の医療現場は限定されたIT・セキュリティリソースを前提にしており、そのような限定性のもとで、地域医療は運営されている点を考慮しないといけないのではないか？	御意見として参考にさせていただきます。
42	情報セキュリティに関する考え方の整理	企画管理編（Management）	１２．１ サイバーセキュリティ対応計画の策定	P46	経産省のサイバーGLではマネジメント層がセキュリティ予算の確保を行うべきとあるため、セキュリティ予算の確保をマネジメント層の責務と定義しないと、そもそも経済産業省のガイドラインとの整合性が取れない。なぜ経営管理編も含めて、セキュリティ予算の確保を行うことはマネジメント層という上位層の責務である点を示さないのか？	ご指摘を踏まえ、経営管理編において、安全管理対策の実施に必要となる資源（予算・人材等）の確保が重要である旨を追記しました。
43	情報セキュリティに関する考え方の整理	企画管理編（Management）	１２．２ サイバーセキュリティ対応計画の実践	P46	医療機関の診療モデル・ユースケースはバラバラなため、＜年次＞はあくまで例示とすべきではないか？	御意見として参考にさせていただきます。
44	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．２．１ 医療機関等の職員による外部からのアクセス	P18	『チャネル・セキュリティ』という表現の定義を明確にすべき。	用語集に定義を示しています。
45	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．１ 不正ソフトウェア対策	P22	EDRやふるまい検知には触れているが、セキュリティ業界の常識としての不正ソフトウェア対策ツールの位置付けを簡単に、概念的にでも紹介すべき。具体的にはEDR・ふるまい検知以外にも、AntiVirus、NextGerationAntiVirus、EndPointProtection、ひいてはNetwork Detection & Response等が存在する。	御意見として参考にさせていただきます。
46	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．２ 情報機器等の脆弱性への対策	P23	『重要なセキュリティに関する情報は、「内閣サイバーセキュリティセンター（NISC）」や「独立行政法人 情報処理推進機構」などが定期的に公表している。これらの情報を確認するほか、必要に応じて利用する情報機器等やソフトウェアを提供する事業者に対応を確認するなどして、最新の情報の入手を図ることが重要である。』との記載については、例えば事業者とリモートメンテナンスを契約した場合に事業者資産としてのリモート機器が導入され、この脆弱性が放置される懸念があることが想定されるため、医療機関としては、「ベンダが病院に持ち込む機器等についても脆弱性対応を求めるよう恒常的に監視すべき」というトーンで記載すべきではないか。	御意見として参考にさせていただきます。

47	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．３ 端末やサーバの安全な利用の管理	P23	『企画管理者は、業務での必要性や利便性などと勘案して、利用する情報機器等や医療情報システムの稼働時間等を整理して、適切な設定を行うことが求められる』とある点は、システム運用編ではなく企画管理編に明記すべきではないか。	御意見として参考にさせていただきます。
48	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	TLS1.2/TLS1.3等の細かい技術的な仕様に依存した記載にて、なぜTLSの細かいバージョンを論じているのか不明。	御意見として参考にさせていただきます。
49	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	P37	境界防御とゼロトラスト思考の整理は、あまりに単純化されすぎている。金融庁が公表している同種のゼロトラレポートも踏まえ、内容への理解を医療分野関係者にも誘導すべきではないか。	御意見として参考にさせていただきます。
50	情報セキュリティに関する考え方の整理	システム運用編（Control）	１４．認証・認可に関する安全管理措置	P41	【遵守事項】-⑥-『医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること』との記載は、昔ながらの表現をそのまま転用することは望ましくなく、現行の技術動向を考慮し、こうしたパターンは想定されるのかという観点から検討すべき。	御意見として参考にさせていただきます。
51	情報セキュリティに関する考え方の整理	システム運用編（Control）	１８．外部からの攻撃に対する安全管理措置	P48	「サイバー攻撃にあったら、バックアップデータ使ってもそこにマルウェア感染しているかも。それを使って復旧しても感染拡大するかもだから注意して」といった概略的な記載は被害を受けた病院として何をやるべきか具体的に記載すべき。	御意見として参考にさせていただきます。
52	情報セキュリティに関する考え方の整理	他(参考資料)	Ｑ＆Ａ （案） 経Ｑ-９	P13	少人数で運営されている場合は費用の捻出が難しく、実際には「第三者に外部監査を依頼することが」難しい可能性が高いように思われる。その場合監査人に選ばれた担当者はシステムやセキュリティに関する知識が不足する場合に備え、助けになるようにチェックリストを提示する等、担当者に依存しない確認方法を示した方が良いのではないか。	御意見として参考にさせていただきます。
53	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	P39	EDRはエンドポイント対策でありエージェントのインストールが必要である事からインストールできないIoT機器は対象外となってしまうため、トラフィックを監視可能なNDRとした方が適切かと思われる。	御意見として参考にさせていただきます。
54	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	P38	「ゼロトラスト思考の有効性は、認められるものの、これを実装するためには、現時点では費用や管理に対する負担が大きいとされており、医療機関等においても小規模の医療機関等で導入することは必ずしも容易ではない。」 の表現はゼロトラストに否定的な印象。特に医療機関においては境界内での利用が大半なので、境界型防御の中にゼロトラストの概念を組み入れたセキュリティ対策をとって行くかは重要かと思われます。	御意見として参考にさせていただきます。
55	情報セキュリティに関する考え方の整理	システム運用編（Control）	―	―	Windowsサーバのビルトインアカウントであるadministratorは、ユーザーIDは公知のものでかつパスワードを間違えてもアカウントロック出来ない。システム運用編において、このような特権IDが乗っ取られるランサムウェア被害の防止策として特権IDの管理について言及すべきかと思われる。	御意見として参考にさせていただきます。
56	情報セキュリティに関する考え方の整理	概説編（Overview）	２．３ 医療情報システムの範囲	P2	「なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。」は、複数の解釈ができてしまう可能性がある。サイバーセキュリティは、「医療情報」を扱っているかではなく、医療の継続に重要であるかどうかが重要な観点であり、さらに、医療情報を扱うことを想定していないシステムにおいても、医療情報を扱うシステムとの接続、同一ネットワーク内での同居等もあり得ることから、「なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まないが、しかし、それが医療の継続提供に著しい影響を与えるおそれのある場合はサイバーセキュリティ対策の対象になり得る。医療情報を扱うシステムと同一ネットワークに接続する医療情報を扱わない機器に関しても留意が必要である。」と変更して欲しい。	御意見として参考にさせていただきます。
57	情報セキュリティに関する考え方の整理	経営管理編（Governance）	【はじめに】	P1	攻撃が高度化、巧妙化されたことよりも、それなしでも対策が十分でないことが課題で、対策が十分だと思っていても、攻撃の高度化、巧妙化でさらに強化が必要なことを記載すべきではないか。 (変更案) 「対策が十分に行われていなかったことで、医療機関等の経営や地域医療の安全性に直接影響が生じる事案も生じている。さらに、その攻撃手法は日々高度化、巧妙化しており、確実な対策とその強化が求められている。」	御意見として参考にさせていただきます。
58	情報セキュリティに関する考え方の整理	経営管理編（Governance）	１．２．２ 非常時における責任	P5	＜善後策を講ずる責任＞に、原因究明、再発防止、通常時の準備はあるのですが、復旧に関しての記載がない。	御指摘を踏まえ、非常時において、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図る必要がある旨を追記しました。
59	情報セキュリティに関する考え方の整理	経営管理編（Governance）	２．１ 医療情報システムにおけるリスク評価の実施	P9	（リスクの回避・低減・移転・受容） は、最近のISMS等に合わせて「移転」を「共有」にすべきではないか。同様に説明文書内も語句の整合した語句を変更。	御意見として参考にさせていただきます。
60	情報セキュリティに関する考え方の整理	経営管理編（Governance）	３．１．２ 医療情報システムにおける統制上の留意点	P13	「統制の内容を検討すること」は検討ではなく検討したものを実施することが必要。検討することが遵守事項だと、それを説明するのが困難。留意点全てを遵守事項ではなく、3.1.1.の解説に含めてしまったらどうか。	御意見として参考にさせていただきます。
61	情報セキュリティに関する考え方の整理	経営管理編（Governance）	３．４．１ 事業継続計画（BCP：Business Continuity Plan）の整備と訓練	P16	「情報セキュリティインシデントにより、医療機関等内の 医療情報システムの全部又は一部 に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、 当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて、改善に向けた対応を指示すること。」は、回りくどい文章になっている。復旧手順の検討ではなく作成を指示、作成と自己点検及び改善は別な項目にしたほうがわかりやすいのでは。 (変更案) ② 情報セキュリティインシデントにより、医療機関等内の医療情報システムの全部又は一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を策定するよう、企画管理者及びシステム運用担当者に指示すること。 ③ 復旧手順について、随時自己点検を行うように指示し、その結果報告を受けること。必要に応じて、改善に向けた対応を指示すること。	御意見として参考にさせていただきます。

62	情報セキュリティに関する考え方の整理	企画管理編（Management）	８．情報管理（管理、持ち出し、破棄等）	P32	システム運用編７．情報管理（管理・持出し・破棄等）【遵守事項】②で保守業務を行う事業者に対するデータの取扱いについての記載があるため、企画管理編においても、委託者に対するルールとして、データの持ち出しを禁止することを原則とする手順等とするように記載してはどうか。	企画管理編「15⑨技術的な安全管理対策の管理」において、「医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規程等に含めること。」と記載しています。
63	情報セキュリティに関する考え方の整理	システム運用編（Control）	１．情報セキュリティの基本的な考え方	P3	基本的考え方は理解できますが、この遵守事項を実施していることの確認が困難であると思われます。何をすべきかの要件をもう少し具体化して遵守事項に記載すべきであり、それが無理なら本遵守事項は削除すべき。	御意見として参考にさせていただきます。
64	情報セキュリティに関する考え方の整理	システム運用編（Control）	６．１ 安全管理対策に関するシステムアーキテクチャ（クライアント側、サーバ側、インフラ、セキュリティ）	P14	「本ガイドラインでは、これらにつきクライアント側、サーバ側、インフラ、セキュリティとして区分し、それぞれに関する技術的な対応としての遵守事項を整理した。」の記載は、①に記載の項目と本書の章とが一部対応されていない部分があるので対応させるべきでは。 (i) 「情報の持出し・管理・破棄等に関する安全管理措置」vs「情報管理(管理・持ち出し・破棄等) (ii) 「事業者選定と管理」に対する章は存在しない。 (iii) 「インフラ運用管理(通常時・非定常時)」vs「システム運用管理(通常時・非定常時)」 (iv) 「ーインフラ」にも「「インフラ運用管理(通常時・非定常時)」が存在するが「サーバ側」にも存在する。 (v) 16章には「紙媒体等で作成した医療情報の電子化」があるが、6章には記載ない。 (vi) 「証跡のレビュー、システム監査」vs「証跡のレビュー・システム監査」	御意見として参考にさせていただきます。
65	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．利用機器・サービスに対する安全管理措置	P21	「ネットワークの構成分割やネットワーク間のアクセス制御」は非常に重要であるが、遵守事項及びその他の章の遵守事項に本内容の記載が見当たらない。 情報資産を特定し、その資産の特性に合わせて、ネットワーク構成を明確にするとともに、その構成分割、セグメント間のアクセス制御を実施することは非常に重要である。例えば医療機関では、IoTのような医療機器、電子カルテ等の医療情報システム、メール、Webアクセスする端末などの一般IT機器等があり、それぞれをセグメント化してかつ、その間の情報を制御するために機器、ポート等の厳格なフィルタがセキュリティ上重要である。しかし、それらが明確に記載されている箇所が見当たらない。	非常時に備えた論理的/物理的なネットワークの構成分割については、システム運用編「11.システム運用管理」に記載しています。 なお、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」において、医療機関内で医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したネットワーク構成図等を作成する等、ネットワーク環境を整備することが求められています。また、当該手引書では、医療機器の使用環境における新たなリスクや進化するリスクを評価し、適切な緩和策によってリスクをコントロールするために最大限努力する必要があり、この対応策としては、ネットワークのセグメンテーション等が挙げられる旨、記載されています。
66	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．２ 情報機器等の脆弱性への対策	P23	脚注2、3以降にも令和5年3月31日付けで「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」が発出されている。さらに、医療機器を医療機関で使うにあたり「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」も発出されている。	ご指摘を踏まえ修正いたしました。
67	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	医療機関等内部での「ネットワークの構成分割やネットワーク間のアクセス制御」などの遵守事項を明確に記載すべきではないか。情報資産を特定し、その資産の特性に合わせて、ネットワーク構成を明確にするとともに、その構成分割、セグメント間のアクセス制御を実施することは非常に重要である。例えば医療機関では、IoTのような医療機器、電子カルテ等の医療情報システム、メール、Webアクセスする端末などの一般IT機器等があり、それぞれをセグメント化してかつ、その間の情報を制御するために機器、ポート等の厳格なフィルタがセキュリティ上重要である。 さらにクラウドを使用した場合にそのクラウドに接続するための医療機関内部でのネットワーク構成等が重要で、クラウド事業者の責任外になる可能性が高い。	非常時に備えた論理的/物理的なネットワークの構成分割については、システム運用編「11.システム運用管理」に記載しています。 なお、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」において、医療機関内で医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したネットワーク構成図等を作成する等、ネットワーク環境を整備することが求められています。また、当該手引書では、医療機器の使用環境における新たなリスクや進化するリスクを評価し、適切な緩和策によってリスクをコントロールするために最大限努力する必要があり、この対応策としては、ネットワークのセグメンテーション等が挙げられる旨、記載されています。クラウド事業者に関するご意見については、参考とさせていただきます。
68	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１．２ 選択すべきネットワークのセキュリティ	P37	SSL-VPNについての記載は「導入が容易である反面、偽サーバへの接続リスク等があり対策が必要とされる」が正しい表現ではないか。	御意見として参考にさせていただきます。
69	情報セキュリティに関する考え方の整理	システム運用編（Control）	１４．認証・認可に関する安全管理措置	P41	（設定ファイルにパスワードが記載される等があってはならない）の記載は、設定ファイルに暗号化されて記述されている分には問題がないことから（設定ファイルにパスワードが平文で記載される等があってはならない）ではないか。	ご指摘を踏まえ修正いたします。
70	情報セキュリティに関する考え方の整理	経営管理編（Governance）	１．２．２ 非常時における責任	P5	「経営管理編」では非常時において、原因や対策などの説明責任や原因を究明し、発生経緯の整理や再発防止策など善後策を講じる責任が求められ、また「企画管理編」でも非常時にはリスク低減や被害拡大防止の対応策を講じる責任が求められている。より具体的な事例を掲載することが、セキュリティ対策の第一歩または強化を促し、本ガイドラインの実効性を高めることに繋がると考えるため、ガイドラインの実効性を高めるために、経済産業省所管のサイバーセキュリティお助け隊などのセキュリティ商材やサイバー保険などを「具体的な対策事例」として記載して欲しい。	御意見として参考にさせていただきます。
71	情報セキュリティに関する考え方の整理	経営管理編（Governance）	２．２．１ リスク評価を踏まえたリスク管理	P10	医療機関等において選択される主なリスク管理方針である「低減」策の一つとしてサイバー保険の活用も考えられることから、サイバー保険はリスク管理手法の「低減」策の一つである旨、記載することが適当であると考える。	御意見として参考にさせていただきます。

72	情報セキュリティに関する考え方の整理	企画管理編（Management）	１１．３ 非常時の事象が生じた際の対応	P43	「経営管理編」では非常時において、原因や対策などの説明責任や原因を究明し、発生経緯の整理や再発防止策など善後策を講じる責任が求められ、また「企画管理編」でも非常時にはリスク低減や被害拡大防止の対応策を講じる責任が求められている。より具体的な事例を掲載することが、セキュリティ対策の第一歩または強化を促し、本ガイドラインの実効性を高めることに繋がると考えるため、ガイドラインの実効性を高めるために、経済産業省所管のサイバーセキュリティお助け隊などのセキュリティ商材やサイバー保険などを「具体的な対策事例」として記載して欲しい。	御意見として参考にさせていただきます。
73	情報セキュリティに関する考え方の整理	すべて	－	－	メールセキュリティの国際標準であるDMARCの導入について言及がないのは、非常に問題。	御意見として参考にさせていただきます。
74	情報セキュリティに関する考え方の整理	すべて	－	－	一般医療従事者等によるパスワードの使い回しによる、メールアカウントの大量漏洩等による被害等に関して、最低限のリテラシ教育等について（経営者の責務として）記載すべき。	利用者認証にパスワードを用いる際の具体的な留意点については、システム運用編「１４．認証・許可に関する安全管理措置」に記載しています。
75	情報セキュリティに関する考え方の整理	経営管理編（Governance）	－	－	セキュリティ予算の確保について一切触れていない点は実効性の確保という観点で大きな問題である。	ご指摘を踏まえ、経営管理編に、安全管理対策の実施に必要となる資源（予算・人材等）の確保に努めることが重要である旨を追記しました。
76	情報セキュリティに関する考え方の整理	経営管理編（Governance）	３．４．２ 情報共有・支援、情報収集	P17	「EOS(End of Sale,Support,Service)」の記載は、厚労省発行のIMDRFサーバーセキュリティガイダンス、ガイダンスの各手引書（医療機器向け、医療機関向け）では、医療機器でのEOSは“End of Support”に限定して使用されていることと平仄を合わせるべきではないか。なお、システム運用編8.2でも同様の記載がある。	御意見として参考にさせていただきます。
77	情報セキュリティに関する考え方の整理	すべて	－	－	医療機器のサイバーセキュリティに関しては、「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」を実施するよう通知され、それと対になる医療機関での対応は、「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」に示されたが、安全管理ガイドライン第6版の案においては、これらが全くふれられていない。医療機関は、安全管理ガイドライン第6.0版とともに、「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」を両方実施することを要求されているのか。	システム運用編「8.2情報機器等の脆弱性のへの対策」に記載の通り、医療機器については「医療機器のサイバーセキュリティ導入に関する手引書」等を踏まえて医療機器の製造販売業者と必要な連携を図ることも求められると考えます。
78	情報セキュリティに関する考え方の整理	すべて	－	－	医療機関内においては、医療機器のセキュリティ維持、確保のためにZone等のネットワークのセグメント設計をしっかりした上での設置、使用が望まれる。医療機関内部のネットワーク、ルーティング、セグメント等を、接続される機器の特性を加味して設計するようなことをもっと明確化すべきではないか。 さらに、最近はクラウド等の活用も多く、クラウド事業者のセキュリティだけではなく、医療機関内からクラウドに接続するための院内のネットワーク構成等が非常に重要となる。クラウド事業者は、医療機関の外に関しては責任範囲にする可能性が高いが、医療機関の内部に関しては責任範囲の外になる可能性が高いため、このあたりをもっと医療機関が注目してもらうようにしてもいいのではないか。	「医療機関における医療機器のサイバーセキュリティ確保のための手引書」において、医療機関内で医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したネットワーク構成図等を作成する等、ネットワーク環境を整備することが求められています。クラウド事業者に関するご意見については、参考とさせていただきます。
79	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置 １３．３．１ ネットワーク回線の暗号化	P39	遠隔医療における動画や音声などのリアルタイム通信ではTCPベースのHTTPS/TLSではなくDTLSやSRTPといったUDPベースのプロトコルが適している場合が多く、これらのプロトコルも十分な強度で暗号化されており、クライアント認証の上での接続も実現できることから、医療情報を安全に取り扱うことができると考えているため、HTTPS/TLS以外での接続として、例えばDTLSやSRTPについても利用可能であることをガイドラインもしくは関連するQA等にて示していただきたい。	DTLSやSRTPについては脆弱性の発見が続いていることから、原案通りとさせていただきます。
80	情報セキュリティに関する考え方の整理	企画管理編（Management）	３．１．５ 非常時の体制・CSIRT 等の整備	P18	運用管理編において必要な文書の体系を「方針、規程、規則、マニュアル類、各種資料」と定義しているので、ガイドライン全体で共通用語とすべくここで使用されている「手順等」の文字は「マニュアル等」に変更してはどうか。	御意見として参考にさせていただきます。
81	情報セキュリティに関する考え方の整理	企画管理編（Management）	１０．運用に対する点検・監査	P39	本章は運用に対する要求だと思われ、【遵守事項】②③④は下記の通りに変更してはどうか。 ② 医療情報システムの運用を委託している場合は、 ③ 医療情報システムの運用に関する点検結果を、 ④ 医療情報システムの運用の安全管理の状況を客観的に把握するために、	御意見として参考にさせていただきます。
82	情報セキュリティに関する考え方の整理	企画管理編（Management）	１２．サイバーセキュリティ	P45	本編４．１で「規程→規則→マニュアル等及び各種資料」で具体化されると説明しているので、【遵守事項】③の「各規程や手順等に反映すること。」は「各規程や規則等に反映すること。」としてはどうか。	御意見として参考にさせていただきます。
83	情報セキュリティに関する考え方の整理	システム運用編（Control）	１７．証跡のレビュー・システム監査	P47	誤操作の修正対応は、改ざん防止とは分けて考えていただきたい。	御意見として参考にさせていただきます。
84	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１ ネットワークに対する安全管理	P36	これまでのガイドラインでは「公衆網」として含まれていた「携帯網等」の該当箇所がないため、図１２－２ 本ガイドラインにおけるネットワークの整理の「専用線」に「専用線・回線事業者による回線サービス」として「回線事業者による回線サービス」に「携帯網等」を含ませる記載がふさわしい。 また、上記考え方をＱ＆Ａにて補記を行ったほうがより理解が促進されると考える。	御意見として参考にさせていただきます。
85	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	P37	「多層防御」の趣旨として、境界防御を複数のセグメントに施し、多層にするという考え方と、境界防御に加えトラフィック監視等の技術的対策を施し、多層にするという考え方があると考えられ、システムの実装・運用を担う担当者への理解を促すため、「多層防御の考え方」について、具体的な考え方・対策（多段・多層での防御）をＱ＆Ａにて補記いただきたい。	御意見として参考にさせていただきます。

86	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	0	最後のパラグラフ「さらに、」から始まる文は、以下理由より（変更案）を提案する。 ・境界防御だけではなく、境界内部に侵入した攻撃に対する内部対策は非常に重要な不正対策。 ・内部対策の具体的な方法としてはEDRと併せて、境界防御として前段に記載されているファイアウォール機能を内部対策にも活用したマイクロセグメンテーションという仕組みやIDS/IPSを内部対策に利用する事も、極めて有効な具体的な対策方法。 ・EDRに加えて、それらファイアウォールやIDS/IPSを内部対策の具体的な対策方法として明記することで、システム担当者のセキュリティ対策に対する具体的な取り組みが促進され、一層有効な不正対策が実現できる。 （変更案） 「さらに、外部からのサイバー攻撃の高度化・多様化に鑑みると、境界防御の対策を行っていたとしても、不正ソフトウェア等の攻撃や侵入があることから、このような場合を想定して、内部脅威監視 やEDRなどの措置を講じることも、有効な対策として挙げられる（「8.1 不正ソフトウェア対策」 参照）。なお、ファイアウォールやIDS/IPSなどのシステムは、境界防御だけではなく内部脅威の対策としても有効であるため、内部ネットワーク上での不正な攻撃の検知および遮断をするシステムとしての採用も検討する必要がある 。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。」	御意見として参考にさせていただきます。
87	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	オンプレのみとなっているが、クラウドも対象になっていなくてよいのか。または、クラウドに関して、「経産省・総務省から発行されているガイドラインを参照することする。」でよいのか。	システム運用編「13.ネットワークに関する安全管理措置」については、クラウド型を採用している場合は参照を省略できます。
88	情報セキュリティに関する考え方の整理	システム運用編（Control）	１７．証跡のレビュー・システム監査	P47	オンプレだけではなく、クラウドシステムも対象となるのか。	医療情報システムの構成に応じて、事業者に確認のうえ、事業者と締結する契約等に含まれている場合は、簡略化が可能です。
89	情報セキュリティに関する考え方の整理	経営管理編（Governance）	１．２．２ 非常時における責任	P5	現場の IT 部門だけでなく、 経営層や法務部門等を含めた方針策定が必要であるとの観点から、経営管理編の医療機関等における責任に、サイバー犯罪者が利益を得て、違法な目的を助長することを防ぐ「社会的責任（倫理規定）」を含めるべく、【遵守事項】＜善後策を講ずる責任＞に「④これらの施策は。法令等を遵守し身代金要求などサイバー犯罪者に毅然と立ち向かい、社会的責任に努めること。」の追記を提案します。	御意見として参考にさせていただきます。
90	情報セキュリティに関する考え方の整理	企画管理編（Management）	１１．１ 非常時における対応方針の策定 １１．２ 非常時に備えた通常時からの対応	P40	現場の IT 部門だけでなく、 経営層や法務部門等を含めた方針策定が必要であるとの観点から、経営管理編の医療機関等における責任に、サイバー犯罪者が利益を得て、違法な目的を助長することを防ぐ「社会的責任（倫理規定）」を含めること、又業務上の判断を行うにあたり、先入観をもたず、他者からの不当な影響を受けず、常に公正な立場を堅持し、公正・誠実に業務を遂行し、毅然とした態度で対応すべく以下２点の追記を提案する。 ・「１１．１ 非常時における対応方針の策定」の３行目「災害やサイバー攻撃、システム障害が生じて非常時となった場合に、」の下ポツ２の下に、「・法令や社会的責任等を配慮し復旧及び再発防止をどのように対策するか」の追記。 ・「１１．２ 非常時に備えた通常時からの対応」の５行目「サイバー攻撃においては、耐攻撃性や業務継続性という観点から対応が必要となる。」を「サイバー攻撃においては、耐攻撃性や業務継続性という観点と、法令等を遵守し身代金要求などサイバー犯罪者に毅然と立ち向かう対応が必要となる。」に修正。	御意見として参考にさせていただきます。
91	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．２．２ 患者等に診療情報等を提供する場合の外部からのアクセス	P19	患者は自身のデータしか閲覧できず、かつ、自身のデータを漏洩させるモチベーションは非常に低いということを考えると、３パラの「ネットワーク対策等に関しては、基本的には「７．２．１　医療機関等の職員による外部からのアクセス」に示すものと同様の対策を講じることが求められる。」のような不特定多数の患者のデータにアクセスできる医療従事者と同様に仮想デスクトップのような技術の導入を求める記載は過剰であると考えます。	患者等に診療情報等を提供する場合の外部からのアクセスについては、システム運用編7.2.2において、「なお、患者への情報提供は、一般的には参照のみとなること、患者等においては職員以上に単純な仕組みが求められることなどを考慮して、対応策を検討することが求められる。」と記載のとおり、セキュリティ確保の仕方について医療機関において適切に判断いただきたいと考えています。
92	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．情報管理（管理・持出し・破棄等）	P16	全国の医療・介護施設が利用するクラウドサービスへのアクセスにおいて、仮想デスクトップ（のような）技術を用いてアクセスすることを標準とするのは無理があると考えられることから、【遵守事項】⑬は「本来、クローズドなLAN内での利用が主である情報システム」への外部からのアクセスを想定していると想定すると、「外部からのアクセスを許可する」対象のシステムを明確にしたほうがよいのではないか。	御指摘を踏まえ、VPNと組み合わせた仮想デスクトップに技術を限定しないような書きぶりに修正いたしました。
93	情報セキュリティに関する考え方の整理	企画管理編（Management）	１５．技術的な安全管理対策の管理	P55	医療機関等の施設外からのアクセスについては「システム運用編」７．２章にて医療機関等の職員が訪問先やテレワークなどで医療機関外から医療機関側の端末にアクセスする場面が想定されていることから、原文にあるような入退室管理される区画で端末を操作することはできないと思われ、【遵守事項】②の「医療機関等の施設外からの入力・参照等が可能な端末等についても同様である」は、「医療機関等の施設外からの入力・参照等が可能な端末等については運用管理規程等を策定し、関係者に周知徹底すること」にした方がよい。	外部端末からのアクセスについては企画管理編第8章に記載があります。ご指摘の趣旨を踏まえ、「医療機関等の施設外からの入力・参照等が可能な端末等についても同様である」の文言は削除します。
94	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．２ 情報機器等の脆弱性への対策	P23	医療機関向けに、医療機器のサイバーセキュリティに関して求められる手引書が3月31日に発行されており、医療機関はその内容を把握する必要があると考えられることから、最後のパラグラフは、『本ガイドラインにおいては、医療情報の適切な保全を目的としてIoT機器の適切な取扱いに関する要件を定めているものであり、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」1において定める医療機器のサイバーセキュリティの保全については、厚生労働省医薬・生活衛生局から発出されている「医療機器におけるサイバーセキュリティの確保について」2、「医療機器のサイバーセキュリティの確保に関するガイダンス」3、「医療機関における医療機器のサイバーセキュリティ導入に関する手引書について」等を踏まえて、医療機器の製造販売業者と必要な連携を図ることも求められる。』にした方がよい。	ご指摘を踏まえ修正いたしました。
95	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	【遵守事項】②の「オープンではないネットワーク」という語は、ここでで初出のため、単に「オープンなネットワーク」（インターネット）の対語と認識され、オープンなネットワークを活用したインターネットVPNやSSL VPNは含まれない（=IP-VPNと専用線のみが原則と指定されている）、と解釈されてしまうことから、「セッション乗っ取り、 IPアドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること」と修正してはどうか。	ご指摘を踏まえ修正いたしました。

96	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	【遵守事項】⑧⑨において、第5.2版での記載では、当該の要件は、【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】という条件下で求められていたが、本案での記載では前提とする条件が不明確なため、【遵守事項】⑧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）医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。」、【遵守事項】⑨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）ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん 及び中間者攻撃等を防止する対策を実施すること。」とした方がよい。	御意見として参考にさせていただきます。
97	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１ ネットワークに対する安全管理	P35	【遵守事項】⑬の「利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること。」は、当該文章の目的が無線LAN通信の確保なのか、無線LAN以外の通信に対する干渉の防止なのかが不明確であることから、「利用する無線 LAN の電波特性を勘案して、通信を阻害するものを設置しないこと。」または「利用する無線 LAN の電波特性を勘案して、通信が阻害されないものを利用すること。」にした方がよい。	御意見として参考にさせていただきます。
98	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１ ネットワークに対する安全管理	P35	図１２-１にISDNの単語の記述があるが、ガイドラインの文書の説明分に一度もISDNの記述がない、またサービスも2023年一杯で終了するので省いた方がよいと思われる。	御意見として参考にさせていただきます。
99	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１．２ 選択すべきネットワークのセキュリティ	P37	「IPsec+IKE で実現するVPN と SSL VPN がある。」 という表現では、オープンなネットワークであるインターネットを用いるサービスとしてIPsecもしくはSSL VPNしか使用できないと解釈される恐れがあり、第5.2版の「IPsecもしくは新たな技術によりそれと同等以上の安全性が担保されているVPN」という表現に戻すべく、 「オープンなネットワークであるインターネットを用いるサービスとしては、IPsec+IKEで実現するVPNとSSL VPNがある。」を 「オープンなネットワークであるインターネットを用いるサービスとしては、IPsec+IKEで実現するVPN、SSL VPN等がある。」 「システム運用担当者は、基本的にはIPsecなど安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画等の方針なども踏まえて、適切なものを選択することが求められる。」を「システム運用担当者は、基本的には IPsec、WireGuard、OpenVPNといった安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画等の 方針なども踏まえて、 適切なものを選択することが求められる。」 とした方がよい。	御意見として参考にさせていただきます。
100	情報セキュリティに関する考え方の整理	他(参考資料)	Ｑ＆Ａ （案） シＱ－14	P69	クラウド型電子カルテでブラウザ等を利用しＰＣ上に情報が残留しない運用で、TLS1.2+証明書により通信経路の安全性を確保して運用している場合、往診など院外にて、ノートPC等から仮想デスクトップを利用せず、クラウド型電子カルテ利用を行うことは問題ないか。	ご提案の方法は本ガイドラインの内容に反するものではありません。
101	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．情報管理（管理・持出し・破棄等）	P16	仮想デスクトップ相当の技術は医療機関等の施設側において仮想環境を用意するためのCPU性能およびメモリ容量等の必要リソース増加を伴うこと等、医療機関等にコスト負担増を強いることになる上、その技術だけに限定する必然性が見い出せないこと等は元より、第5.2版では6.11.D.1として推奨項目だったものが今般においては【遵守事項】⑬と必須要件化されているため、遵守事項から除外し、Q&Aにおける例示に留めるべきではないか。	御指摘を踏まえ、VPNと組み合わせた仮想デスクトップに技術を限定しないような書きぶりに修正いたしました。
102	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１．２ 選択すべきネットワークのセキュリティ	P37	「IPsec+IKE で実現するVPN と SSL VPN がある。」 という表現では、オープンなネットワークであるインターネットを用いるサービスとしてIPsecもしくはSSL VPNしか使用できないと解釈される恐れがあり、第5.2版の「IPsecもしくは新たな技術によりそれと同等以上の安全性が担保されているVPN」という表現に戻すべく、 「オープンなネットワークであるインターネットを用いるサービスとしては、IPsec+IKEで実現するVPNとSSL VPNがある。」を 「オープンなネットワークであるインターネットを用いるサービスとしては、IPsec+IKEで実現するVPN、SSL VPN等がある。」 「システム運用担当者は、基本的にはIPsecなど安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画等の方針なども踏まえて、適切なものを選択することが求められる。」を「システム運用担当者は、基本的には IPsec、WireGuard、OpenVPNといった安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画等の 方針なども踏まえて、 適切なものを選択することが求められる。」 とした方がよい。	今後の検討事項とさせていただきます。
103	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．１ 不正ソフトウェア対策	P22	EDR（Endpoint Detection and Response）の有用性について説明内容を拡充した方が良い。	御意見として参考にさせていただきます。
104	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．２ 情報機器等の脆弱性への対策	P22	「医療情報システムが利用する情報機器等の脆弱性に関する情報を常に収集し、脆弱性への対応を速やかに行う必要がある。」については、部門システムなど導入に関連する会社が多岐にわたるため、システム運用者が人為的に情報を集めて精査を行い、利用する情報機器等を提供する事業者に個別に確認作業を行うことは非常に困難。	御意見として参考にさせていただきます。
105	情報セキュリティに関する考え方の整理	システム運用編（Control）	１７．証跡のレビュー・システム監査	P47	「全てのアクセスログを収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。」の記載は、システム運用者が手作業でこれらを洗い出すことは不可能であると考えられ、具体的な手法を例示していただきたい。	例えば、医療機関等の規模によっては、ログ管理システムを導入すること等も想定できます。
106	情報セキュリティに関する考え方の整理	システム運用編（Control）	４．リスクアセスメントを踏まえた安全管理対策の設計	P10	HELICS標準の積極採用を推進するために【遵守事項】②の例として、HELICS標準になっている「HS040「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド」も追加してはどうか。	御意見として参考にさせていただきます。
107	情報セキュリティに関する考え方の整理	システム運用編（Control）	１２．物理的安全管理措置	P31	第5.2版(6.4.物理的安全対策)時にＤ項であった「情報管理上重要な区画に防犯カメラ、自動侵入監視装置等を設置すること。」が【遵守事項】②とされているのは過剰な対策になっていると思われる。	御意見として参考にさせていただきます。
108	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．１ ネットワークに対する安全管理	P36	図１２-２の後の説明では、接続先等の管理がなされていないネットワークを「オープンなネットワーク」とし、「IKE+IPsec接続」を「セキュアなネットワーク」としているが、【遵守事項】⑥からは「IKE+IPsec接続」は「オープンなネットワーク」の中で使用するものとされていることから図中の「オープンなネットワーク」は「セキュアでないネットワーク」とした方が適切であり、「セキュアでないネットワーク」においてもOSI４層以上のレイヤにおいてチャネルセキュリティが確保できる通信方式（たとえばTLS1.3の利用など）については許容できることについてＱ＆Ａにて詳述するべき。	御意見として参考にさせていただきます。

109	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．利用機器・サービスに対する安全管理措置	P21	「サイバーセキュリティに関する情報」がどのような情報かの説明がどこにもないため、【遵守事項】⑥の「サイバーセキュリティ」は「情報セキュリティ」とするか、「サイバーセキュリティに関する情報」を具体的に解説欄もしくはＱ＆Ａで説明して欲しい。	サイバーセキュリティに関する情報とは、情報機器等の脆弱性に関する情報を想定しています。
110	情報セキュリティに関する考え方の整理	―	―	―	医療情報管理体制加算の要件である「医療情報システム安全管理責任者」（安全管理責任者）や「システム運用管理責任者」（運用管理責任者）が本文書中で明確に定義されていない。情報セキュリティの一般的な考え方に照らすと、安全管理責任者はCISO（Chief Information Security Officer）に、運用管理責任者はCISO補佐に当たる方とすると、CISOは経営管理層で業務に当たる方で、CISO補佐は組織の形態（兼任関係）によって、本文で示される「企画管理者」であったり、「担当者あるいはシステム運用管理者」であったりするものと考えられることから、 ・経営管理編の３．１．１の統制に関する遵守事項において「管理体制等を整備」を「医療情報システム安全管理責任者を配置した管理体制等を整備」と、「医療情報システム安全管理責任者」を明記して欲しい。 ・概説編の「2.本ガイドラインの対象」等に新たに項目を設け、兼任関係に応じて、安全管理者、運用管理責任者、企画管理者、担当者またはシステム運用管理者との関係性を明確にし、合わせて、概説編の図3-1等に現れる用語の定義や考え方を整理して明記してほしい。 ・企画管理編の「３．１．５非常時の体制・CSIRT等の整備」の文中にCISOの配置を企画管理者が検討するように求める記述は、経営管理層の人材配置を企画管理層の人物が検討するのは適切では無いとの考えから、「企画管理者はこれらの整備の要否や、必要な場合にはその構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」を「企画管理者はCSIRTの構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」と修正いただきたい。	ご指摘を踏まえ、経営管理編において、医療情報システム安全管理責任者にかかる記載を追記しました。また、「企画管理者」と「システム運用管理者」という文言が混在していたため、「企画管理者」に統一いたしました。
111	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．情報管理（管理・持出し・破棄等）	P16	【遵守事項】⑬は例示を増やすことにより導入を推進しやすくするためにも、総務省テレワークセキュリティガイドラインにも記載されている例示に倣い、「利用者による外部からのアクセスを許可する場合は、 利用する端末 の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップやセキュアブラウザ、セキュアコンテナのような技術を用いるとともに、運用等の要件を設定すること。」としてはどうか。	御指摘を踏まえ、VPNと組み合わせた仮想デスクトップに技術を限定しないような書きぶりに修正いたしました。
112	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．１ 外部へ持ち出す医療情報の管理対策	P17	持ち出し端末による医療情報システムへのアクセスをパスワードのみの認証で行わせるのはリスクが大きいとの考えから、２パラは「記録媒体や情報機器等を持ち出す場合には、盗難や紛失のリスクを想定した内容を含めることが求められる。例えば持ち出し端末自体の起動時には、端末の二要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証の仕組みを実装することを原則必須とし、認証等のルールに沿った内容であることが求められる。また記録媒体や端末内に患者等の医療情報が保存されている場合には、記録媒体やHDDに暗号化を施す必要がある。記録媒体や端末自体に医療情報が保存されておらず、アクセス先にのみ患者等の医療情報が存在する場合は、その機能を持つアプリ利用時の認証と、端末起動時の認証を組み合わせて二要素認証とすることも考えられる（異なる二要素である必要がある）。」としてはどうか。	ご指摘の点については今後の検討にあたっての参考にさせていただきます。
113	情報セキュリティに関する考え方の整理	システム運用編（Control）	７．２．１ 医療機関等の職員による外部からのアクセス	P18	最後の「したがって、」から始まる一文は、例示を増やすことにより導入を推進しやすくするためにも、総務省テレワークセキュリティガイドラインにも記載されている例示に倣い、「したがって、職員による外部からのアクセスを行う場合は、利用するPC等の端末 の作業環境内に仮想的に安全管理された環境を VPN技術と組み合わせて実現する仮想デスクトップやセキュアブラウザ、セキュアコンテナのような技術の導入を検討するなどの対応が求められる。」としてはどうか。	ご指摘の趣旨を踏まえ「仮想デスクトップあるいは同等以上の安全性を確保できる方法を用いる」に修正しました。
114	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．利用機器・サービスに対する安全管理措置	P21	【遵守事項】⑤においては、総務省や内閣サイバーセキュリティセンター（NISC）からパスワードを定期変更する必要はないとの話も出ており対策の選択肢を示すためにも、「情報機器の利用方法等に応じて必要があれば、二要素認証もしくは定期的なパスワードの変更等の対策を実施すること。」としてはどうか。	御指摘を踏まえ、VPNと組み合わせた仮想デスクトップに技術を限定しないような書きぶりに修正いたしました。
115	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．３ 端末やサーバの安全な利用の管理	P23	パスワード設定以外を例示することにより、対策の推進をしやすくするためにも２パラは「安全な利用については、８．１、８．２に示す対策のほか、例えば情報機器の起動にパスワード等の設定や二要素認証を行うなど、必要な措置を講じることが求められる。」としてはどうか。	御意見として参考にさせていただきます。
116	情報セキュリティに関する考え方の整理	―	―	―	情報セキュリティを確保する上での医療情報システムの範囲は、会計を扱うシステムも各種の医療機器も含めて適切に管理する必要があることから、 ①概説編「２．３ 医療情報システムの範囲」の最初の一文は「本ガイドラインが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、当該情報システムに接続される医療機器を含め、医療情報を扱う情報システム全般を想定する。」とし、 ②２パラのなお書きは「なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、システム単体では、本ガイドラインにおける医療情報システムには含まれないが、医療情報を扱う情報システムと接続する限りにおいては、本ガイドラインの安全管理の対象に含まれる。」 ③概説編の「４．３ 医療情報システムの安全管理に関連する法令」と、「４．４ 医療情報システムに関する統制」の最終段落に「医療機器のサイバーセキュリティ導入に関する手引書」を追記。 ④企画管理編「９．医療情報システムに用いる情報機器等の資産管理」【遵守事項】①のなお書きを「なお、情報機器等には、医療情報システムに用いる情報機器や当該システムに接続する医療機器といった物理的な資産のほか、医療情報システムが利用するサービス、ライセンスなども含む。」としてはどうか。	御意見として参考にさせていただきます。なお、医療情報システムの範囲については、Q&A（概Q-5）に記載があります。
117	情報セキュリティに関する考え方の整理	システム運用編（Control）	８．５ 医療機関等が管理する以外の情報機器の利用に対する対策	P24	「管理者が定期的に確認すること等」においては例示を増やすことにより導入を推進しやすくするため、「管理者が定期的に確認することやセキュアブラウザ、セキュアコンテナのような技術を導入することなど、適切な対策を選択・採用し、十分な安全性が確保された上で行う必要がある。」としてはどうか。	御意見として参考にさせていただきます。

118	情報セキュリティに関する考え方の整理	―	―	―	医療情報システムの安全性を一定以上に維持するために、「企画管理者」や「担当者またはシステム運用管理者」は、対処するべきリスクとその考え方を示せば適切な技術選択が可能な情報技術に明るい者である必要があり、その者が適切な技術選択をできるようにするためにも、本改定の趣旨に則り本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであることから、企画管理編３．１．１の文末に「企画管理者は、これらの対応を自ら行うことにたる、医療情報システム・情報技術に関する十分な知識や理解を有する必要がある。」を追記し、３．１．４ の一文目は「～技術的な対応を行う担当者（医療情報システムの安全管理のうち技術的な対応を自ら行うにたる、情報技術に関する十分や知識や技能を有する者）」と補記した上で、システム運用編において以下の各項目に記載された具体的技術的手段についてＱ＆Ａに移し、当該項目では方法の一例を一般論として記載できる範囲に留めるよう記載を修正してはどうか。 ・７【遵守事項】⑬：「VPN・仮想デスクトップ」を廃し、「端末の作業環境内に医療情報が残存することが無いようにする」等の記述に変更。 ・７【遵守事項】⑭：「TLS暗号化、PKI認証等」を「暗号化、認証等」に変更。 ・７．２．１：詳細な記載を廃し「チャネルセキュリティを確保し、BYODにおいては端末の作業環境内に医療情報が残存することが無いようにする」に変更。 ・７．２．２：患者が自らの情報のみにアクセスする際と職員が不特定の患者情報にアクセスする際のセキュリティはリスク評価が大幅に異なり、同列の対応を求めるのは技術的に正しくないことから当該項目の第三段落を削除。 ・８【遵守事項】⑤：個別技術としての起動時パスワード設定のみを求めることは不適当であるので、当該項目を削除。 ・８【遵守事項】⑥：IoT機器のみに特化した詳細な記述を廃し、①～⑤に記述されていない(3)のみを一般的な情報端末の事項として記述。 ・８．５：「管理されていない端末でのBYODは行わない。」以下の、個人所有物を組織が管理するという論理的に実施不可能な対策を削除。 ・１３．【遵守事項】④：「採用する認証手段は」以降の具体的技術に関する記載を削除 ・１３．【遵守事項】⑥：IPSec、HTTPS、TLS、クライアント証明書等の技術用語を廃し、「オープンなネットワークにおいて仮想専用線（VPN）を用いる場合には、安全性の高い暗号を用い、セッション間の回り込み等による攻撃に対して適切な対策を実施すること。」など一般的な事項のみを記載するように変更。	システム運用編では、医療機関等において経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の設計、実装、運用等を担う担当者を対象としたものであり、具体的な技術については、必要な範囲で例示として言及することにより、適切な選択を促し、安全管理の取組を推進するという観点から、ご指摘の点については原案通りとさせていただきます。
119	情報セキュリティに関する考え方の整理	システム運用編（Control）	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置	P26	昨今共通のアカウント・パスワードを利用していることが原因で不正アクセスのインシデントが発生していること又「１４．１．１ 利用者の識別・認証」に「認証を実施するためには、医療情報システムへのアクセスを行う全ての職員及び関係者に対し ID・パスワードや IC カード、電子証明書、生体認証等、本人の識別・認証に用いる手段を用意し、医療機関等の内部で統一的に管理する必要がある。」の記載があり、リモートメンテナンス（保守）においてはより強固に二要素認証を導入することにより、不正アクセスを防ぐ必要があると考えることから、【遵守事項】③は「保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントおよび二要素認証を使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。」としてはどうか。	御意見として参考にさせていただきます。
120	情報セキュリティに関する考え方の整理	システム運用編（Control）	―	―	医療情報システムの安全性を一定以上に維持するために、「企画管理者」や「担当者またはシステム運用管理者」は、対処するべきリスクとその考え方を示せば適切な技術選択が可能な情報技術に明るい者である必要があり、その者が適切な技術選択をできるようにするためにも、本改定の趣旨に則り本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであることから、システム運用編において以下対応が必要と考えます。 ・【遵守事項】⑬：WPA2-AES、WPA2-TKIP等の技術用語を廃し、「医療情報システムにおいて無線LANを利用する場合、適切な利用者以外に無線LANを利用されないようにし、不正な情報の取得を防止するため適切な暗号化を施し、通信が阻害されることのないようにすること。」など一般的な事項のみを記載。 ・１３．１．２：技術解説的文書である、第2、第3、第4段落を全て廃し、第5、第6を「システム運用担当者は、適切な仮想専用線（VPN）を選定する、あるいは、事前に事業者との契約を確認するなどし、チャネル・セキュリティが確実に確保されるようにしておく必要がある。」など一般的な事項のみを記載。 ・１３．２：ゼロトラスト思考に関する一般的解説文書である表12-1及び第1、第2段落及び最終段落を廃し、タイトルに即し「医療情報システムと外部情報ネットワークとの境界においてだけではなく、情報システム内部においても、適切なリスク分析に基づき、トラフィックの監視等の対策を講じることが重要である。」など一般的事項のみを記載。 ・１３．３．１：TLS、SSL-VPN等の技術用語を廃するよう変更。 ・１４【遵守事項】⑤：認証を強固にする技術の一つに過ぎず、かつ、システム運用上の多大な障害になり得る二要素認証を遵守事項とするのは適切で無いことから削除。 ・１４．１．１：二要素認証を過大評価している第5段落以降を廃止、「二要素認証等の認証強度が強いとされる認証方式を導入する事も求められる。」等に変更。 ・１４．１．２：外部アプリケーションとの連携方式はRESTに限られないことから、「昨今、システム間連携の」以降の文を廃し、第2段落の「API連携の」を「外部アプリケーションとの接続時の」に変更。	御意見として参考にさせていただきます。
121	情報セキュリティに関する考え方の整理	他(参考資料)	［特集］ 医療機関等におけるサイバーセキュリティ（案）	―	医療情報システムの安全性を一定以上に維持するためには、想定する読者である「企画管理者」や「担当者 または システム運用管理者」は、対処するべきリスクとその考え方を示せば適切な技術選択が可能である程度の、情報技術に明るい者で無くてはなりません。これらの担当者が適切な技術選択をできるようにするためには、本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであると考えることから、「[特集]医療機関等におけるサイバーセキュリティ(案)」に記載されている事項は、「企画管理者」や「担当者 または システム運用管理者」が当然読まねばならない他の情報セキュリティ文書に預け、廃するのが適切ではないか。	昨今医療機関を対象としたランサムウェア等のサイバー攻撃事案が発生し、その脅威が高まっていることから、本特集においては、ガイドライン中のサイバーセキュリティに関係する部分を要約するとともに、具体例を盛り込むことで、医療機関等の対策に役立てていただくべく作成したものであり、原案通りとさせていただきます。

122	情報セキュリティに関する考え方の整理	他(参考資料)	Ｑ＆Ａ　（案）	―	医療情報システムの安全性を一定以上に維持するためには、想定する読者である「企画管理者」や「担当者 または システム運用管理者」は、対処するべきリスクとその考え方を示せば適切な技術選択が可能である程度の、情報技術に明るい者で無くてはなりません。これらの担当者が適切な技術選択をできるようにするためには、本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであると考えることから、Ｑ＆Ａにおいて一般的な情報セキュリティに関する事項については記載せず、医療情報システムの安全管理や医療分野における情報セキュリティ特有の事項に絞った記述にすることが適切ではないか。	今後の検討にあたっての参考とさせていただきます。
123	情報セキュリティに関する考え方の整理	経営管理編（Governance）	１．２ 医療機関等における責任	P4-5	医療機関の非常時に対応すべき責任は非常に重要な事項ではあるものの、医療者に求められるのは医療サービス提供の継続と医療安全を最優先にする姿勢であり情報セキュリティは決して医療安全に優先しないとの考えから、表１−１ 医療機関等における責任の「情報セキュリティインシデントの原因・影響等に関する説明責任」の上に、「患者の生命・身体への影響を考慮し、医療継続を図る責任」という大前提事項であるを明記し、１．２．２【遵守事項】＜説明責任＞①の書き出しを「情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について」と改訂してはどうか。	ご指摘を踏まえ、経営管理編 1.2.2 遵守事項において、情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るべき旨を追記しました。
124	情報セキュリティに関する考え方の整理	―	―	―	経営管理編３．３．２では情報セキュリティ監査を受けうる必要があることを又同編２．２．２ではISMSの実践を謳っており、その一環として監査をうけることが文全体の整合性を考えると適切であると考えることから以下追記をしてはどうか。 ・経営管理編３．３．２の第２項「外部機関による監査」に続いて「ISMS更新審査など」を追記。 ・企画管理編３．１．８の１パラ「外部の第三者による方法」に続いて「ISMS更新審査を受審する方法など」を追記。	御意見として参考にさせていただきます。
125	情報セキュリティに関する考え方の整理	企画管理編（Management）	８．情報管理（管理、持ち出し、破棄等）	P32 P33	情報セキュリティの考え方として、情報を外部からアクセスさせるようにして情報の持出を禁ずることが医療情報の紛失・漏示等の事故を防ぐために効果的であることから、【遵守事項】⑧に「医療機関等において保有する医療情報の医療機関外への不適切な持ち出しが発生しないよう、医療機関は医療機関外から保有する医療情報に安全にアクセスできる手段を、医療従事者や職員等に提供することに努めねばならない。」を、また、８．１．１ 情報管理方針の整備 の１パラの後に、「医療機関等において保有する医療情報の医療機関外への持ち出しや、それに伴う情報漏示が発生する可能性を少なくするよう、医療機関は医療機関外から保有する医療情報に安全にアクセスできる手段を、医療従事者や職員等に提供することに努める必要がある。」と追記するのはどうか。	御意見として参考にさせていただきます。
126	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P35	【遵守事項】⑬ の１つめは、無線LANにおける利用者認証に最適な方法を記載することで対策を推進しやすくするため「適切な利用者以外に無線 LAN を利用されないようにすること。例えば、認証サーバを利用したWPA2/WPA3エンタープライズによる認証(IEEE802.1X認証)を採用する等の対策を実施すること。」としてはどうか。	御意見として参考にさせていただきます。
127	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．４ 無線 LANの利用における対策	P40	無線LANにおける利用者認証に最適な方法を記載することで対策を推進しやすくするため、２パラは「無線LAN は無線を用いたネットワークであることから、適切な措置を講じないと本来利用が許されない 第三者の利用が生じるほか、侵入者による攻撃などを招くリスクがある。また適切な暗号化を講じないと、盗聴や不正ソフトウェアの混入などのリスクも生じるため、例えば、認証サーバを利用したWPA2/WPA3エンタープライズによる認証（IEEE802.1X認証）を採用する等の対策を実施すること。」としてはどうか。	御意見として参考にさせていただきます。
128	情報セキュリティに関する考え方の整理	企画管理編（Management）	８．情報管理（管理、持ち出し、破棄等） １５．技術的な安全管理対策の管理	P32 P55	診療録管理は、ナースステーション等院内の多くの場所でのアクセスが可能であり、これを閉鎖空間として標記の管理をするなどは非現実的かつ今後のさらなる医療DXを進めるためにも、「入退室管理」「施錠」にかかる記載については、現状に即した運用ができるような記載に変更すべき。	御意見として参考にさせていただきます。なお、ナースステーションにおける入退室管理についてはQ&A（企Q-54）に記載があります。
129	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	端末IDやセキュリティキーを利用した認証等、技術の進化によりクライアント証明書以外にもクライアント認証をする方法が増えているかと思われ、【遵守事項】⑥は「クライアント証明書等を利用したTLS クライアント認証を実施すること」と表現が適切。	今後の検討事項とさせていただきます。
130	情報セキュリティに関する考え方の整理	システム運用編（Control）	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置	P26	【遵守事項】⑥の書きぶりはSaaSサービスにおいてシステム障害が発生した場合、個別に医療機関様へ許可をいただくことができないことも想定されるが、どのような対応が望ましいのか。	障害時や緊急を要する脆弱性対応などにおいては、事後承認などによることも想定されるが、個人情報の取扱も含め、保守に関する手続きについては原則として事前申請・承認を得ることが望ましいと考えます。
131	情報セキュリティに関する考え方の整理	システム運用編（Control）	―	―	本編の読者は、医療機器を管理する部門担当者が多く含まれると想定されることから、厚生労働省「医療機関における医療機器のサイバーセキュリティ確保のための手引書」との整合性についても触れながら記述されてはどうか。	安全管理ガイドラインで記載されている内容の一部は、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」にも記載されている内容と整合性を持たせたものとなっております。整合性について記述すべきとのご意見につきましては、今後の参考とさせていただきます。
132	情報セキュリティに関する考え方の整理	システム運用編（Control）	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置	P26	【遵守事項】④の記載は、緊急での対応等で必ずしも計画書を事前に作成が困難な場合もあると想定され、「作業を行う前に、保守作業者と実施内容について合意し、作業結果について、報告を受け、記録として残すこと」等としてはどうか。	御意見として参考にさせていただきます。なお、保守に関する手続きは原則として事前申請・承認ですが、障害時や緊急を要する場合には事後承認等によることも想定される旨を、10.1に記載しています。

133	情報セキュリティに関する考え方の整理	企画管理編（Management）	６．２ ISMS（Information Security Management System：情報セキュリティマネジメントシステム）	P25	診療所等の小規模医療機関においては、医療情報部等のシステム運用担当者がいないことでISMS構築のための文書作成や体制を構築することが困難なケースが考えられることから、小規模な医療機関においては、「特集：小規模医療機関等向けガイダンス」の参照を促す文言を追加いただけないか。	御意見として参考にさせていただきます。なお、Q&A（概Q-9）で、小規模医療機関においては「特集：小規模医療機関等向けガイダンス」を参照してほしい旨を記載しています。
134	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．２ 不正な通信の検知や遮断、監視	P37	医療機関のサイバー攻撃対策の一助となるセキュリティ対策として、ネットワークの不正なふるまいを検知することが可能な「NDR(Network Detection and Response)」をガイドラインの不正な通信の検知や遮断、監視の要件として検討に加えていただきたい。	御意見として参考にさせていただきます。
135	情報セキュリティに関する考え方の整理	すべて	―	―	以下箇所において、サポートが終了したソフトウェアへの対策について、買い替えることやネットワークに接続しないことなど具体的な対応内容を記載してはどうか。 ・経営管理編（案）：３．４．２ 情報共有・支援、情報収集 ・企画管理編（案）：９．２ 情報機器等の安全性の確認 ・システム運用編（案）：８．２ 情報機器等の脆弱性への対策	御意見として参考にさせていただきます。
136	情報セキュリティに関する考え方の整理	―	―	―	医療情報管理体制加算の要件である「医療情報システム安全管理責任者」（安全管理責任者）や「システム運用管理責任者」（運用管理責任者）が本文書中で明確に定義されておりません。情報セキュリティの一般的な考え方に照らすと、安全管理責任者はCISO（Chief Information Security Officer）に、運用管理責任者はCISO補佐に当たる方とすると、CISOは経営管理層で業務に当たる方で、CISO補佐は組織の形態（兼任関係）によって、本文で示される「企画管理者」であったり、「担当者あるいはシステム運用管理者」であったりするものと考えられることから、 ・概説編の「2.本ガイドラインの対象」等に新たに項目を設け、兼任関係に応じて、安全管理者、運用管理責任者、企画管理者、担当者またはシステム運用管理者との関係性を明確にし、合わせて、概説編の図3-1等に現れる用語の定義や考え方を整理して明記してほしい。 ・経営管理編の３．１．１の統制に関する遵守事項において「管理体制等を整備」を「医療情報システム安全管理責任者を配置した管理体制等を整備」と、「医療情報システム安全管理責任者」を明記して欲しい。 ・企画管理編の「３．１．５非常時の体制・CSIRT等の整備」の文中にCISOの配置を企画管理者が検討するように求める記述は、経営管理層の人材配置を企画管理層の人物が検討するのは適切では無いとの考えから、「企画管理者はこれらの整備の要否や、必要な場合にはその構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」を「企画管理者はCSIRTの構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」と修正いただきたい。	ご指摘を踏まえ、経営管理編において、医療情報システム安全管理責任者にかかる記載を追記しました。また、「企画管理者」と「システム運用管理者」という文言が混在していたため、「企画管理者」に統一いたしました。
137	情報セキュリティに関する考え方の整理	―	―	―	本改定の趣旨に則り本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであることから、システム運用編において以下の各項目に記載された具体的技術的手段についてＱ＆Ａに移し、当該項目では方法の一例を一般論として記載できる範囲に留めるよう記載を修正してはどうか。 ・７【遵守事項】⑬：「VPN・仮想デスクトップ」を廃し、「端末の作業環境内に医療情報が残存することが無いようにする」等の記述に変更。 ・７【遵守事項】⑭：「TLS暗号化、PKI認証等」を「暗号化、認証等」に変更。 ・７．２．１：詳細な記載を廃し「チャネルセキュリティを確保し、BYODにおいては端末の作業環境内に医療情報が残存することが無いようにする」に変更。 ・７．２．２：患者が自らの情報のみにアクセスする際と職員が不特定の患者情報にアクセスする際のセキュリティはリスク評価が大幅に異なり、同列の対応を求めるのは技術的に正しくないことから当該項目の第三段落を削除。 ・８【遵守事項】⑤：個別技術としての起動時パスワード設定のみを求めることは不適当であるので、当該項目を削除。 ・８【遵守事項】⑥：IoT機器のみに特化した詳細な記述を廃し、①～⑤に記述されていない(3)のみを一般的な情報端末の事項として記述。	システム運用編では、医療機関等において経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の設計、実装、運用等を担う担当者を対象としたものであり、具体的な技術については、必要な範囲で例示記載することにより、適切な選択を促し、安全管理の取組を推進するという観点から、ご指摘の点については原案通りとさせていただきます。

138	情報セキュリティに関する考え方の整理	―	―	―	本改定の趣旨に則り本文中に具体的技術を記載することを極力避け、Q&Aに例示するに留めることを徹底すべきであることから、システム運用編において以下の各項目に記載された具体的技術的手段についてＱ＆Ａに移し、当該項目では方法の一例を一般論として記載できる範囲に留めるよう記載を修正してはどうか。 ・１３．【遵守事項】④：「採用する認証手段は」以降の具体的技術に関する記載を削除 ・１３．【遵守事項】⑥：IPSec、HTTPS、TLS、クライアント証明書等の技術用語を廃し、「オープンなネットワークにおいて仮想専用線（VPN）を用いる場合には、安全性の高い暗号を用い、セッション間の回り込み等による攻撃に対して適切な対策を実施すること。」など一般的な事項のみを記載するように変更。 ・【遵守事項】⑬：WPA2-AES、WPA2-TKIP等の技術用語を廃し、「医療情報システムにおいて無線LANを利用する場合、適切な利用者以外に無線LANを利用されないようにし、不正な情報の取得を防止するため適切な暗号化を施し、通信が阻害されることのないようにすること。」など一般的な事項のみを記載。 ・１３．１．２：技術解説的文書である、第2、第3、第4段落を全て廃し、第5、第6を「システム運用担当者は、適切な仮想専用線（VPN）を選定する、あるいは、事前に事業者との契約を確認するなどし、チャネル・セキュリティが確実に確保されるようにしておく必要がある。」など一般的な事項のみを記載。 ・１３．２：ゼロトラスト思考に関する一般的解説文書である表12-1及び第1、第2段落及び最終段落を廃し、タイトルに即し「医療情報システムと外部情報ネットワークとの境界においてだけではなく、情報システム内部においても、適切なリスク分析に基づき、トラフィックの監視等の対策を講じることが重要である。」など一般的事項のみを記載。 ・１３．３．１：TLS、SSL-VPN等の技術用語を廃するよう変更。 ・１４【遵守事項】⑤：認証を強固にする技術の一つに過ぎず、かつ、システム運用上の多大な障害になり得る二要素認証を遵守事項とするのは適切で無いことから削除。 ・１４．１．１：二要素認証を過大評価している第5段落以降を廃止、「二要素認証等の認証強度が強いとされる認証方式を導入する事も求められる。」等に変更。 ・１４．１．２：外部アプリケーションとの連携方式はRESTに限られないことから、「昨今、システム間連携の」以降の文を廃し、第2段落の「API連携の」を「外部アプリケーションとの接続時の」に変更。	御意見として参考にさせていただきます。
139	情報セキュリティに関する考え方の整理	概説編（Overview）	２．３ 医療情報システムの範囲	P2	情報セキュリティを確保する上での医療情報システムの範囲は、会計を扱うシステムも各種の医療機器も含めて適切に管理する必要があることから、最初の一文は「本ガイドラインが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、当該情報システムに接続される医療機器を含め、医療情報を扱う情報システム全般を想定する。」としてはどうか。	御意見として参考にさせていただきます。なお、医療機器については、別途「医療機器のサイバーセキュリティ導入に関する手引書」（令和５年３月31日薬生機審発0331第11号・薬生安発0331第4号）等を踏まえた対応が必要となります。
140	情報セキュリティに関する考え方の整理	概説編（Overview）	２．３ 医療情報システムの範囲	P2	２パラのなお書きは、「なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、システム単体では、本ガイドラインにおける医療情報システムには含まれないが、医療情報を扱う情報システムと接続する限りにおいては、本ガイドラインの安全管理の対象に含まれる。」としてはどうか。	御意見として参考にさせていただきます。
141	情報セキュリティに関する考え方の整理	他(参考資料)	［特集］ 医療機関等におけるサイバーセキュリティ（案）	―	「[特集]医療機関等におけるサイバーセキュリティ(案)」に記載されている事項は、「企画管理者」や「担当者 または システム運用管理者」が当然読まねばならない他の情報セキュリティ文書に預け、廃するのが適切ではないか。	昨今医療機関を対象としたランサムウェア等のサイバー攻撃事案が発生し、その脅威が高まっていることから、本特集においては、ガイドライン中のサイバーセキュリティに関係する部分を要約するとともに、具体例を盛り込むことで、医療機関等の対策に役立てていただくべく作成したものであり、原案通りとさせていただきます。
142	情報セキュリティに関する考え方の整理	他(参考資料)	Ｑ＆Ａ （案）	―	Ｑ＆Ａにおいて一般的な情報セキュリティに関する事項については記載せず、医療情報システムの安全管理や医療分野における情報セキュリティ特有の事項に絞った記述にすることが適切ではないか。	今後の検討にあたっての参考とさせていただきます。
143	情報セキュリティに関する考え方の整理	経営管理編（Governance）	３．４．３ 情報セキュリティインシデントへの対応体制	P18	情報セキュリティインシデントが対応した場合は、利用しているシステム関連事業者とは関係の無い情報セキュリティインシデント対応の専門家が入り中立的な意見を取り入れ、復旧のコストと期間が短くなるような判断をする体制を取るように促す一文を記載してはどうか。	御意見として参考にさせていただきます。
144	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P34	昨今多くの被害を出しているVPN装置に対しての必要な対策を促すべく、「インターネットもしくは、フレッツ網、多くの加入者のあるIP-VPNで利用するVPN機器は常に脆弱性を残さないように、更新が公開されてすぐに適応する必要があります。また、安易なパスワードや標準のパスワード、ITベンダーが設置したパスワードが容易なものであった場合は変更をする必要があります。」等を追記してはどうか。	御意見として参考にさせていただきます。
145	情報セキュリティに関する考え方の整理	システム運用編（Control）	１３．ネットワークに関する安全管理措置	P35	不正アクセス対策を強化すべく、【遵守事項】⑬に以下を含ませてはどうか。 （記載案） 「不正な情報の取得防止と接続制限ため、WPA3,WPA2-EnterpriseもしくはWPA2-PSK（AES/TKIP）により通信を暗号化すること。パスワードは14文字以上の大文字小文字数字記号を含むパスワードを付けること。」	御意見として参考にさせていただきます。
146	情報セキュリティに関する考え方の整理	すべて	―	―	患者個人の情報に関するものについて外部保存を認める記録等が示されていたりするが、クラウドといっても外部の事業者であり、そこにデータを置く事は、個人情報保護・セキュリティ的に問題となるものであり、全体的に、個人情報を含む医療情報システムのデータについては、クラウドには存在させないべきと考える。	御意見として参考にさせていただきます。
147	外部委託、外部サービスの利用	概説編（Overview）	４．７ 医療情報の外部保存	P10	「医療情報システム・サービス事業者に一部の業務を委託する方が、結果として安価でより安全な情報セキュリティ対策を講じることが可能となることも…」 とあるが、高価でもより安全な方を採用するべきと考えると”安価”という言葉は削除が望ましいのではないか。また、サービス事業者にコストダウンを強要しているようにも読み取れ、結果として委託先の手抜きのきっかけになることが危惧されガイドラインの主旨から外れてしまう。	ご指摘踏まえ修正いたしました。

148	外部委託、外部サービスの利用	企画管理編（Management）	７．安全管理のための人的管理	P28	遵守事項-⑥-[f. プライバシーマーク認定又はISMS認証を取得していること]は、経産省・総務省の２省GLで最低限のセキュリティ適格性に該当しているため、取得要件を最低限必要のものとして確認すべきという位置づけにしないと現行の２省GLとの整合が取れない。そのうえで、最低限の適格性を満たす事業者のセキュリティ成熟度として、⑥にあるその他の資格要件等が定義されるべきであり、そうでないなら、２省GLとの整合性が取れていないロジックの合理性をしっかり本ガイドラインで説明すべき。	ご指摘を踏まえ、Q&A（企Q-27）において、プライバシーマークやISMS認証は医療情報を取り扱う医療情報システムサービス事業者として最低限取得すべきものである旨の考え方を追記いたします。
149	外部委託、外部サービスの利用	企画管理編（Management）	７．安全管理のための人的管理	P28	遵守事項-⑥-[g. 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]にISMAPやJASAのCSゴールドマークの記載がある。一方で、これらの認証は、外部保存の改正通知やe-文書法（電子保存の３原則）への対応を意味するものではなく、単に＜一般的なサイバーセキュリティ/プライバシー対応が出来ている＞ことを保証するのみであり、国内医療セキュリティとの整合性は限定的。 よって、列記する認証を取っていても必ずしも医療セキュリティ適合性には該当しないという留意点を病院関係者にも示す補足を追記すべきではないか。	御意見として参考にさせていただきます。
150	外部委託、外部サービスの利用	企画管理編（Management）	７．安全管理のための人的管理	P28	遵守事項-⑥-[g. 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]に、認証が確認できない場合システム監査技術者あるいはCISA資格取得者による外部監査をすることとの記載があるが、一般社団法人医療情報安全管理監査人協会（iMISCA)が認定する＜医療情報システム監査人＞等の資格はシステム監査技術者 or CISA同等とみなすべきではないか？	御意見として参考にさせていただきます。
151	外部委託、外部サービスの利用	企画管理編（Management）	７．安全管理のための人的管理	P28	遵守事項-⑦-[「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・・・]との記載は、「匿名化した情報」とは現行の個人情報保護法では存在しない概念であるため（匿名加工情報 or 仮名加工情報しか法的定義はない）、「匿名化した情報」とは何なのかについて具体的に定義すべき。	御意見として参考にさせていただきます。
152	外部委託、外部サービスの利用	企画管理編（Management）	７．５ 外部保存・外部委託の終了	P30	『患者の医療情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索履歴等も厳正な取扱いの後に破棄されなければならない』について、想定している具体的なユースケースを明記して欲しい。	御意見として参考にさせていただきます。
153	外部委託、外部サービスの利用	システム運用編（Control）	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置	P26	遵守事項-④-は、少なくとも、リモートメンテの機器の脆弱性対応が十分図られている点についてを補足すべき。理由があって記載していないならその旨を記載すべき。	保守要員が外部機器を持ち込む場合の確認事項については、Q&A（シQ-25）に示しています。
154	外部委託、外部サービスの利用	すべて	ー	ー	不特定多数の小規模組織を対象とするサービス事業者が展開するSaaSとしては、単独では本ガイドラインラインの要件を満たせない可能性(体制の整備等)が考えられるが、その場合は当該の医療機関等ではサービスの利用は不可となるか。それとも、サービス事業者側で肩代わりすることで要件を充足したとすることが可能か。	各編の冒頭に図示しているとおり、クラウド型であって、事業者と締結する契約書に含まれている場合には、当該箇所の参照を簡略化することができるとしています。
155	外部委託、外部サービスの利用	他(参考資料)	Ｑ＆Ａ （案） 企Q-10、企Q-11	P22	システムベンダがSaaSとして不特定多数の医療機関等へサービス提供を行う際、システムの監査等、同一の確認を複数の医療機関等にて実施される場合においては、医療機関等の実施事項として記載されている内容についてシステムベンダ側で実施した結果を、サービス利用している医療機関等へ提示することで充足できないか。 （複数医療機関等で実施される同一の作業内容を、システムベンダにて実施することで、医療機関等の作業量増加を必要最低限とできないか。）	御意見として参考にさせていただきます。
156	外部委託、外部サービスの利用	経営管理編（Governance）	１．２ 医療機関等における責任	P4	(1) 通常時において、非常時の計画及びその訓練が追加必要では。 (2) 非常時において、応急処置、拡大防止及び復旧が追加必要では。 (3)第三者に委託する場合　受託事業者を管理する責任が追加必要。 (4)第三者に医療情報を提供する場合　第三者が適切かを判断する責任、 第三者が適切に管理しているかを管理する責任なども追加が必要では。 表の項目追加に合わせて各遵守事項に関しても追加が必要。	御意見として参考にさせていただきます。
157	外部委託、外部サービスの利用	企画管理編（Management）	２．２．２ 委託における責任分界（複数事業者が関与する場合を含む）	P15	クラウドサービスの利用のときに漏れる可能性が大きいのはクラウドに接続する医療機関内のネットワーク等の設定部分である。クラウドを利用することにより、そのクラウドへの接続の医療機関等の口が脆弱になる可能性が高い。	御意見として参考にさせていただきます。
158	外部委託、外部サービスの利用	システム運用編（Control）	３．責任分界	P5	「から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。」の記載は、 「提供された情報の内容が正確であるかどうかなどを事業者に確認すべきではなく、事業者はそれでなくても常に適切な情報を提供する。 (変更案) 「～から必要な情報等の収集を行うとともに、不明点があれば事業者に確認すること。」	御意見として参考にさせていただきます。
159	外部委託、外部サービスの利用	システム運用編（Control）	３．２ 要求仕様適合性の確認を踏まえた調整	P5	クラウドの場合の設定等に関しては、責任が不明確になりやすい点は記載のとおり。ほかクラウドにした場合に責任が不明確になりやすい点として、医療施設内でのクラウド接続に伴うネットワーク、ルーティングの設定及び、接続機器の保守がある。クラウドに接続するために、その接続する機器から又は機器へのデータが流れる必要があり、ネットワークのルーティング、セグメントなどを適切に変更して維持する必要がある。通常、クラウド事業者は、医療機関内のこのような点を責任外にする場合が多い。このため、医療機関等はこれらを確実に自分たちで管理するか、明確にあるベンダー等に委託することが望まれる。これらを明記すべきではないか。	御意見として参考にさせていただきます。

160	外部委託、外部サービスの利用	システム運用編（Control）	３．４．２ 複数の事業者に対する委託を含む場合の責任分界	P8	表3-2に記載されていない類型でよくあり重要なパターンとして、医療機関等がクラウド上で動作するアプリのサービスの提供を受けるクラウドが医療機関等と直接契約する場合がある。表3-2の一番下の類型に近いが、契約ではクラウドサービス事業者Bが医療機関等と契約する。 クラウドサービスA経由でBの使用も含めて契約できればいいが、費用の観点で医療機関等がBとの直接契約をする場合が多い。Bは、医療情報を直接扱わないため、医療機関等の要求を十分考慮できない場合も多いし、Bが大きな企業で個々の医療機関等の要求の対応をしない場合が多い。このような場合に問題になる場合が多いのではないかと思われます。これらの課題を明記した上で、A経由でBを使い、契約もA経由でBとなることが、前記の課題解決につながる旨を記載したほうがいいのではないか。	御意見として参考にさせていただきます。
161	外部委託、外部サービスの利用	企画管理編（Management）	２．１．２ 通常時における責任	P11	ガイドラインを遵守するべきなのは医療機関等であり、システム関連事業者ではないため「遵守」を「対応」にすべき。	御意見として参考にさせていただきます。
162	外部委託、外部サービスの利用	企画管理編（Management）	３．１．１ 医療情報システムの安全管理のための企画管理者の設置	P17	「企画管理者とは、医療情報システムの安全管理を行うために必要な運用管理の管理責任者を指す。」との定義は「運用管理責任者」で良いのではないか。	第6版では「企画管理者」として定義しており、原案通りとさせていただきます。
163	外部委託、外部サービスの利用	システム運用編（Control）	７．３ 医療情報の破棄	P19	「情報機器等の破棄を外部の事業者に委託した場合には、委託先の事業者から破棄に関する証明や証跡の提供などを求めて、確認することが求められる。」の表現では、医療情報ベンダーに対して破棄（廃棄）を求めるように読み取れる。医療機関等が責任を持って、自らが産業廃棄物処理業者と契約し、その業者に然るべき処置を求め、証明や証跡を求めるべきではないか。ガイドライン中に記述が難しければ、Q&Aに廃棄を行えるのは産業廃棄物処理業者であり、医療情報ベンダーではないことを説明すべき。	御意見として参考にさせていただきます。
164	外部委託、外部サービスの利用	企画管理編（Management）	２．２．２ 委託における責任分界（複数事業者が関与する場合を含む）	P15	「表２-１クラウドサービスの提供パターンと責任分界」内のパターン「医療機関等が複数のシステム関連事業者の提供するサービスを組み合わせて利用」の解説は、本文の解説に沿って下記の通りに修正してはどうか。 （変更案）A、B のサービスに連携部分③がある場合は、各①、②の契約内容に責任分界の取り決めを盛り込む必要がある。	御意見として参考にさせていただきます。
165	外部委託、外部サービスの利用	企画管理編（Management）	７．安全管理のための人的管理	P27	【遵守事項】⑤の「外部保存の委託先事業者に、・・・の情報を閲覧させないこと。」は、他の条項に合わせて強制力を強くした言葉にした方が良いと考え、「外部保存の委託先事業者が、・・・の情報を閲覧しないことを遵守させること。」にしてはどうか。	御意見として参考にさせていただきます。
166	外部委託、外部サービスの利用	システム運用編（Control）	１０．医療情報ステム・サービス事業者による保守対応等に対する安全管理措置	P26	【遵守事項】②のみ文末が強い要求になってないため、「診療録等の個人情報の保護を厳格に実施させること。」としてはどうか。	御意見として参考にさせていただきます。
167	外部委託、外部サービスの利用	システム運用編（Control）	３．４．２ 複数の事業者に対する委託を含む場合の責任分界	P8	表３－２「クラウドサービスの提供パターンと責任分界」のパターン「医療機関等が複数の事業者の提供するサービスを組み合わせて利用」2・は、「A・Bの連携が取れるように③の部分についても各①、②の契約内容に盛り込む必要がある。」の文章がふさわしい。	御意見として参考にさせていただきます。
168	外部委託、外部サービスの利用	企画管理編（Management）	８．３．２ 外部保存をシステム関連事業者に委託している場合の対応	P35	「医療機関等においても適切に破棄」の記載は、「委託先事業者においても適切に破棄」が正しいのではないか。または、委託先事業者が医療機関等においても適切に破棄されたことを確認する、という意味か。	医療機関に現存する医療情報についても適切に破棄されたことを確認する必要があるという趣旨です。
169	外部委託、外部サービスの利用	システム運用編（Control）	３．４．１事業者が提供するサービスの類型による責任分界	P7	「このように、」から始まる最後の文は、企画管理者に関することのため企画管理者編に記載するべき。	ご指摘の趣旨を踏まえ、「企画管理者は」を削除しました。
170	外部委託、外部サービスの利用	システム運用編（Control）	３．５ 第三者提供における責任分界	P9	「医療機関等と提供先との間で責任分界を取り決めることになる。」とある一方で「・提供者と利用者が利用するサーバやクラウドサービス等への提供」とあり、医療機関等、提供者、利用者の区別が不明瞭。	ご指摘の趣旨を踏まえ、「提供者と利用者が利用する」を削除しました。
171	外部委託、外部サービスの利用	企画管理編（Management）	１４．１ 法令で定められた記名・押印のための電子署名の要件	P52	企画管理編(案)「１６．紙媒体等で作成した医療情報の電子化」【遵守事項】③に「スキャナで電子化する際には作業責任者による電子署名を行うこと、その電子署名は14章を参照すること」の記載があり、その14章の【遵守事項】①1.(2)には医師等の国家資格が必要な文書に対する電子証明書の要件が記載されているが、スキャン業務を担当するのは医事課などの事務担当が主となると思われます。この為、作業責任者が使用する電子証明書は、14章の【遵守事項】①1.(2)から医師資格等の検証を除いた要件となる理解で正しいか。	ご見解の通りです。
172	外部委託、外部サービスの利用	企画管理編（Management）	２．１．２ 通常時における責任	P11	「サービス仕様適合開示書の提供」は、「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）」も含ませるため「サービス仕様適合開示書等の提供」が良いのではないか。	ご指摘を踏まえ修正いたしました。
173	外部委託、外部サービスの利用	企画管理編（Management）	２．２．２ 委託における責任分界（複数事業者が関与する場合を含む）	P15	医療機関が主体となり、責任分界を明確にしなければ事業者Aと事業者Bの連携をとるための契約事項とすることは困難であるため、表２-１ クラウドサービスの提供パターンと責任分界の説明は「医療機関等は、A、B の連携が取れるように③の部分について、医療機関等及びクラウドサービス事業者間で齟齬が出ないように、医療機関等で調整を行い各①、②の契約内容を互いの連携相手に伝え責任分界を明確にし対策を行う必要がある。」としてはどうか。	御意見として参考にさせていただきます。

174	外部委託、外部サービスの利用	システム運用編（Control）	３．４．２ 複数の事業者に対する委託を含む場合の責任分界	P8	医療機関が主体となり、責任分界を明確にしなければ事業者Ａと事業者Ｂの連携をとるための契約事項とすることは困難であることから、「A、B の連携が取れるように③の部分を各①、②の契約内容を盛り込む必要がある。」は、「医療機関等は、A、B の連携が取れるように③の部分について、医療機関等及びクラウドサービス事業者間で齟齬が出ないように、医療機関等で調整を行い各①、②の契約内容を互いの連携相手に伝え責任分界を明確にし対策を行う必要がある。」に修正いただきたい。	御意見として参考にさせていただきます。
175	外部委託、外部サービスの利用	すべて	―	―	概説編「４．４ 医療情報システムに関する統制 」をはじめとして、医療情報システム・サービス事業者等との責任分界の管理は極めて重要であると考えられ、同項にも書かれている「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」や「医療機器のサイバーセキュリティ導入に関する手引書」の遵守を事業者に求めることについては以下の項目でも改めて遵守するよう明示的に記載してはどうか。 ・経営管理編１．３．１ 委託（第三者委託）における責任 ・経営管理編１．３．２ 委託（第三者委託）における責任分界 ・経営管理編２．２．３ リスク分析を踏まえた要求仕様適合性の管理 ・経営管理編５．２．２ 体制管理 ・企画管理編２．１．１ 医療機関等における責任と責任分界 ・企画管理編３．１．７ 委託等における安全管理の体制	御意見として参考にさせていただきます。なお、「医療機器のサイバーセキュリティ導入に関する手引書」については、薬生機審発0331第11号・薬生安発0331第４号通知において、製造販売業者等に対する周知を行っており、また「医療機関における医療機器のサイバーセキュリティ確保のための手引書」については、医政参発0331第１号・薬生機審発0331第16号・薬生安発0331第８号通知において、医療機関における体制確保を行うよう関係機関・関係団体への周知を行っています。
176	外部委託、外部サービスの利用	概説編（Overview）	２．３ 医療情報システムの範囲	P2	医療情報システムを利用・管理するために、「医療情報システム・サービス事業者」として想定している事業者と別途契約を結ぶにあたり、対象となる事業者の選定に必要な情報をホームページ等に掲載することを検討してほしい。	委託先の事業者選定については、経営管理編5.1、企画管理編7.4にそれぞれ記載しています。
177	外部委託、外部サービスの利用	経営管理編（Governance）	５．１ 事業者選定	P21	５．１．２の事業者選定の基準 には「外部委託において」や「医療情報の取り扱いに関する委託先事業者」の記載があるため、【遵守事項】①②もそれに合わせた書きぶりにしていただけないか。	御意見として参考にさせていただきます。
178	外部委託、外部サービスの利用	経営管理編（Governance）	５．２．１ 契約管理	P22	「委託契約において」だけでは何の委託契約か分からないため、「委託契約において」を「医療情報の取扱いに関する委託契約において」にしてはどうか。	御意見として参考にさせていただきます。
179	外部委託、外部サービスの利用	企画管理編（Management）	２．１．２ 通常時における責任	P11	（１）説明責任の「医療情報システム・サービスの運用等についてシステム関連事業者に委託している場合には・・・」は、 ・クラウドサービスや医療情報を取り扱う運用を委託する場合は2省ガイドラインの「サービス仕様適合開示書」の提供をベンダーに求める。 ・オンプレミスで医療情報を取り扱う運用を委託していないが場合は、MDSで本ガイドラインの適合状況を確認する。 等運用の定義を具体的に示していただけると医療機関とシステム関連事業者での共通理解が深まるのではないか。	御意見として参考にさせていただきます。
180	外部委託、外部サービスの利用	企画管理編（Management）	２．１．４ リスク分析を踏まえた要求仕様適合性の確認への対応	P13	３パラの書き出しにMDSを追記をし、「実際には、システム関連事業者が提供するMDS等の情報やサービス仕様適合開示書等の内容を踏まえて、」としていただけないか。	「サービス仕様適合開示書等」の「等」には、MDS/SDSも含んでいます。
181	外部委託、外部サービスの利用	システム運用編（Control）	３．２ 要求仕様適合性の確認を踏まえた調整	P5	２パラ「例えば、」から始まる文は下記のような文面のほうがより具体的で誤解を与えないのではないか。 「例えば、医療情報の取り扱いを委託する場合やクラウドサービスを利用する際、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」においては・・・その基礎となる内容はサービス仕様適合開示書等により示されている。また、オンプレミスにおいては、日本画像医療システム工業会（JIRA）の工業会規格（JESRA：Japanese Engineering Standards of Radiological Apparatus）及び保健医療福祉情報システム工業会（JAHIS）の JAHIS 標準となっている「『製造業者/サービス事業者による医療情報セキュリティ開示書』ガイド」で示されているチェックリスト等などがある。」	「サービス仕様適合開示書等」の「等」には、MDS/SDSも含んでいます。
182	外部委託、外部サービスの利用	システム運用編（Control）	４．２ リスクアセスメントを踏まえた安全管理対策の設計	P11	事業者より提示する書類は「サービス仕様適合開示書」だけではないことから、途中にあるなお書きは、「なお事業者からは、「サービス仕様適合開示書」や「MDS」などの提示を受けることが想定される。」としてはどうか。	ご指摘を踏まえ、「サービス仕様適合開示書等」と修正します。
183	外部委託、外部サービスの利用	システム運用編（Control）	１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置	P26	【遵守事項】にて、リモートメンテナンス（保守）を行う際のリスクアセスメントの定期的な実施を明示してはどうか。	御意見として参考にさせていただきます。
184	外部委託、外部サービスの利用	経営管理編（Governance）	５．２ 事業者管理	P22	医療機関は機器やソフトウェアの設定、運用状況など実施状況管理監督し安全に保つ立場として、システム関連事業者の設定やセキュリティ上危険な設計思想やガイドライン順守をしないこと等によるセキュリティ侵害は防ぐため【遵守事項】に以下を追記してはどうか。 （追記案） 委託するシステム関連事業者の実施状況を実地で観察し、報告を受け、定期的なアップデートや機器のセキュリティに関する作業が漏れなく、正しく行われているか実施状況の管理を行うように、企画管理者に指示すること。	御意見として参考にさせていただきます。
185	その他・全般	すべて	―	―	実現できる医療機関がどの程度あるのだろうかと疑問。契約書一つとっても、べき論が主で具体論が全くない。	御意見として参考にさせていただきます。
186	その他・全般	すべて	―	―	書いてあることは最もだが、現実的に医療機関のSEのスキル面及びマンパワー面でも対応困難。必要な資格(基本情報技術者以上、医療情報技師など)を求め、病院が資格取得支援や手当を出せる体制を確保しないと実用性がない。	御意見として参考にさせていただきます。
187	その他・全般	他(参考資料)	Ｑ＆Ａ （案） 概Ｑ－１	P2	「システムに関係するベンダや事業者にも本ガイドラインを読んでいただき・・・」との記載は、２省ガイドラインにも似たような内容が複数ガイドラインに記載されており冗長な内容となっている。２省ガイドラインとの重複箇所・範囲についても明記すべきではないか。	御意見として参考にさせていただきます。
188	その他・全般	概説編（Overview）	２．１ 医療機関等の範囲	P1	医療機関等の範囲が「・・・『等』」との記載となっている。本ガイドラインの対象外となるケースの明記又は医療機関等の定義を明確に記載いただきたい。	御意見として参考にさせていただきます。

189	その他・全般	概説編 （Overview）	２．３ 医療情報システムの範囲	P2	『なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理 システム等は、本ガイドラインにおける医療情報システムには含まない』との記載は、あたかも医事会計システムやレセコンも含まれないように見える。業務委託費用の支払い等、業務用途で用いるシステムは含まれないと明記すべき。	御意見として参考にさせていただきます。なお、医療情報システムの範囲については、Q&A（概Q-5）に記載があります。
190	その他・全般	企画管理編 （Management）	１．１．２ 医療情報システムに関係する法令	P5	『企画管理者はこれらの法令等の内容を把握、整理した上で必要な措置を講じることが求められる』とあるが、この節の中で例えば従来のQAで論じていた、医師の診療根拠になる限りにおいて画像データを操作した結果も医療データの一部として管理すべき等の記載がある一方、本体資料にそうした、＜医師の診療根拠・記録根拠に該当する電子データはガイドラインの適用スコープになる＞」点を明示しない理由は何故か。	Q&A（概Q-3）において、このガイドラインの対象となる情報について示しています。
191	その他・全般	システム運用編 （Control）	３．２ 要求仕様適合性の確認を踏まえた調整	P5	『システム運用担当者はこれらの資料を収集し、医療機関等におけるリスク評価との差異などを確認し、必要があれば個別の調整を事業者と行うなどにより、技術的な対応に関するリスク分担などを行うことが求められる』との記載は、病院が事業者にこうした資料の提示を依頼しても対応が行われないケースが非常に多く見受けられるため、事業者のリスクコミュニケーションの協力が得られない状況下で病院はどのような対応を行うべきかの方針を示して欲しい。	御意見として参考にさせていただきます。
192	その他・全般	システム運用編 （Control）	４．２ リスクアセスメントを踏まえた安全管理対策の設計	P11	『利用を想定する事業者において行うリスクアセスメントと、これを踏まえた技術的な対応における対策などを参考にすることなどが考えられる』との記載は、事業者がユーザー（医療機関）の立場より保身を優先した対処にならぬよう、病院はパッシブな立場での確認でなく、事業者が２省ガイドラインに基づき行うリスクマネジメント結果を踏まえて、病院というユーザに依頼すべきセキュリティ実施事項が何であるのかをプロアクティブに求めるべき。	御意見として参考にさせていただきます。
193	その他・全般	システム運用編 （Control）	４．２ リスクアセスメントを踏まえた安全管理対策の設計	P11	『特に専任の情報システムの要員がいない医療機関等の場合には、安全な医療情報システム・サービスを事業者から導入し、構築と運用等は事業者に委ねるほうが、安全性や経済性で優れている』との記載は、あたかも事業者への丸投げ・盲目的な依存を是認するような表現に読める。	御意見として参考にさせていただきます。
194	その他・全般	システム運用編 （Control）	１１．システム運用管理（通常時・非常時等）	P28	遵守事項-①-の『非常時のユーザアカウントや非常時用機能」の手順を整備すること』との記載にある「非常用機能」とは特権ID機能のことであるのなら、安全管理GLの初期段階でインプットとされた、2000年代前半のNEMA等のブレークグラスの考え方をなぜ今も援用するのかが理解しがたく、もしそうでないのなら、「非常時期のユーザアカウント」と「特権ID」の違いについて明示すべき。	御意見として参考にさせていただきます。
195	その他・全般	他(参考資料)	Ｑ＆Ａ （案） 概 Ｑ－５	P4	Q&Aに医療情報システムの範囲に、例えば遠隔で業者が動作状況等を監視するCT・MRIや手術用ロボット等は含まれますか？また、がん登録やNCD等、症例を集めているシステムやその通信に必要なネットワークも含まれますか？	医療情報システムに該当しない医療機器そのものについては本ガイドラインの対象ではありませんが、診断に用いる画像等を電子化して保存する場合は本ガイドラインの対象情報となります。なお、医療機関においては、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」において、医療機器のサイバーセキュリティの確保が求められています。当該手引書は、医療安全についてサイバーセキュリティ上のリスクが懸念される医療機器を対象とします。具体的にはネットワークや機器との接続が可能であるプログラムを用いた医療機器です。また、症例データベース等何らかのかたちで患者の医療情報を保有するコンピューター及びそのネットワークについて、医療機関等が管理するものについては、医療情報システムに該当します。
196	その他・全般	他(参考資料)	Ｑ＆Ａ （案） シＱ－３	P63	MEDISツール開発は過去のことであるため文末表現を過去形に変更してはどうか。 修正案：MEDISでは、前述の相互運用性実証事業において医薬品と臨床検査については、各医療機関が定める独自の用語・コードから標準的な用語、コードにマッピングするためのツールを開発しました。	ご指摘通り修正いたしました。
197	その他・全般	すべて	－	－	レビューの質の向上、効率向上のため配布されるPDFの文書は、最低でもしおり付きPDFにして、可能でしたらWordの原ファイル(変更履歴付き)又はNativeなHTML又はXML＋Readerなどの構成で公開して欲しい。	御意見として参考にさせていただきます。
198	その他・全般	すべて	－	－	文書のルールに関して意識した校正等を徹底し、誰もが読みやすく誤解を招かない方法の記載を考慮すべき。	御意見として参考にさせていただきます。
199	その他・全般	すべて	－	－	Wordの変更履歴付きで前版との違いを公表して欲しい。	前版からは大幅に構成を変更しているため、変更履歴ではなく、項目移行対応表を作成し公表いたします。
200	その他・全般	すべて	－	－	本ガイドラインを利活用したガイドライン等の作成が必要になる。	御意見として参考にさせていただきます。
201	その他・全般	概説編 （Overview）	１．はじめに	P1	本ガイドラインの位置付けをもう少し丁寧に説明すべき。根拠法はe文書法以外に個人情報保護法であり、最近、医療法施行規則の改訂により、医療法も根拠法であうことが明確にされた。以前から医療法が根拠法の1つだが、今回、それが明確にされたことが重要である。	ご指摘を踏まえ、医療法施行規則の改正にかかる記載を盛り込みました。
202	その他・全般	概説編 （Overview）	２．本ガイドラインの対象	P1	「本ガイドラインは、医療機関等において、すべての 医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象とする。」は、2章の対象の1つの観点であることから以下の記載が望ましい。 (変更案) 2. 本ガイドラインの適用範囲 2.1 対象者の範囲 医療機関等において、すべての 医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象とする。 2.2 医療機関等の範囲 ： 2.3 医療情報及び文書の範囲 ： 2.4 医療情報システムの範囲	御意見として参考にさせていただきます。
203	その他・全般	概説編 （Overview）	２．３ 医療情報システムの範囲	P2	「医療情報を保存するシステムだけではなく、 医療情報を扱う情報システム全般を想定する。」は、前半が主要であるような表現のが、より適切ではないか。 (変更案) 「医療情報を保存するシステム、その他医療情報を扱う情報システム全般を想定する。」	御意見として参考にさせていただきます。

204	その他・全般	概説編 （Overview）	４．１．２ 医療情報システムの有用性	P6	医療従事者の負担軽減は容易に理解できますが、患者の負担軽減は、この文脈では不要では。	御意見として参考にさせていただきます。
205	その他・全般	概説編 （Overview）	４．３ 医療情報システムの安全管理に関連する法令	P7	本ガイドラインの位置付けをもう少し丁寧に説明すべき。4.3には医療法及び施行規則も追加しておくべきではないか。	ご指摘を踏まえ、医療法施行規則の改正にかかる記載を盛り込みました。
206	その他・全般	経営管理編 （Governance）	－	－	経済産業省及びIPAによる「サイバーセキュリティ経営ガイドライン」は企業に対して作成されたものであるが、さまざまな分野で整合されたガイドラインを共通言語にすることが望ましい。	御意見として参考にさせていただきます。
207	その他・全般	経営管理編 （Governance）	１．安全管理に関する責任・責務	P3	責任と責務とを両方記載しているが、本文での責務は医療サービスの提供の継続性の確保、維持のみで使われていてそれ以外は責任としているため、タイトルは「・責務」は削除して「責任」だけにしていいのでは。	御意見として参考にさせていただきます。
208	その他・全般	経営管理編 （Governance）	１．１ 安全管理に関する法令の遵守	P3	「法令等を遵守すること。」は当然のことであり経営者の責任としては② に記載があるように遵守させることが重要なため、①を削除したらどうか。	御意見として参考にさせていただきます。
209	その他・全般	経営管理編 （Governance）	１．１．１ 医療情報システムに対する医療機関等の責任	P3	「公的な責務と考えられるため」は、「公的な責務であるため」のように言い切ったほうがより適切ではないか。	御意見として参考にさせていただきます。
210	その他・全般	経営管理編 （Governance）	１．２．１ 通常時における責任	P4	①「原則として文書化し」で「原則として」は削除し、必要に応じて、解説又はＱ＆Ａ等に文書化しない場合の特殊事例、条件などを記載するほうがわかりやすくなるのでは。	御意見として参考にさせていただきます。
211	その他・全般	経営管理編 （Governance）	１．２．１ 通常時における責任	P4	②「患者等への説明を適切に行うための窓口の設置」はわかりにくい。患者の医療データの取扱いに関して、患者に説明できるようになっていればよいのではないか。	御意見として参考にさせていただきます。
212	その他・全般	経営管理編 （Governance）	１．２．１ 通常時における責任	P4	「通常時における説明責任とは、医療情報システムの機能や運用について、必要に応じて患者等に説明する責任である。」は、誤解を招くおそれがある表現ではないか。患者に医療情報システムの機能に関して説明する場合は、ほとんどなく、あくまで、適切に管理されていることを適切な第三者に説明でき、それを患者が理解できることが重要ではないか。	御意見として参考にさせていただきます。
213	その他・全般	企画管理編 （Management）	１．管理体系	P3	「患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。」は誤解を招く表現。「医療情報システムの安全管理」に関する窓口ではなく、医療情報の取扱いに関しての問合せ、苦情に対応する窓口であるべきではないか。	御意見として参考にさせていただきます。
214	その他・全般	他(参考資料)	Ｑ＆Ａ （案） 概Ｑ－１	P2	「安全管理は運用と技術とが相まって一定のレベルを達成するものです」は、今回、安全管理ガイドラインは、「経営編」「企画管理編」「システム運用編」と分離している。このなかで「経営編」の位置付けも明確に記載したほうのがより適切なのではないか。 (変更案) 安全管理は経営の統制のもとに、運用と技術とが相まって一定のレベルを達成するものです	御意見として参考にさせていただきます。
215	その他・全般	他(参考資料)	Ｑ＆Ａ （案） 概Ｑ－11	P7	「厚生労働省として実施しているものはありませんが」としていますが、現時点までの状況等を鑑みると、厚生労働省としても説明会又は研修会等を検討していくべきではないか。	御意見として参考にさせていただきます。
216	その他・全般	他(参考資料)	用語集	P15	BCP[災害時、中でも大規模災害時]と記載されている。昨今は、サイバー攻撃に対してもBCPが要求されているため、それも記載すべきではないか。	御意見として参考にさせていただきます。
217	その他・全般	他(参考資料)	Ｑ＆Ａ （案） 経Ｑ－１	P9	令和5年4月1日から施行されている医療法施行規則第14条第2項の説明も追加すべきではないか。	ご指摘を踏まえ、医療法施行規則の改正にかかる記載を盛り込みました。
218	その他・全般	他(参考資料)	－	－	「医療法施行規則の一部を改正する省令 について」(産情発0310第２号、令和５年３月10日付け厚生労働省大臣官房医薬産業振興・医療情報審議官通知)によると、「なお、安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省において別途 チェックリストを作成し、後日通知する。」と示されていた。このため、チェックリストに関しても早急にパブコメ等を開始していただけるといいのではないかと思われます。	御意見として参考にさせていただきます。
219	その他・全般	すべて	－	－	しおりなしのPDFではなく、最低限しおり付きPDFにしてほしい。	御意見として参考にさせていただきます。
220	その他・全般	すべて	－	－	最終版ではWord版、Excel版、変更履歴付き等の版も公開してほしい。	御意見として参考にさせていただきます。
221	その他・全般	他(参考資料)	Ｑ＆Ａ （案）	－	内容が大量なため第5.2版程度の「目次」が必要。	御指摘を踏まえ目次を作成しました。
222	その他・全般	他(参考資料)	第5.2 版→第6.0版 項目移行対応表（案）	－	5.2 版1～5 章までの対応が省略され過ぎている。	御意見として参考にさせていただきます。
223	その他・全般	すべて	－	－	医療情報システム・サービス事業者の略称の（システム関連事業者への）について、経営管理編ではシステム関連事業者、企画管理編では委託先事業者、システム運用編では情報システム・サービス事業者（以下「事業者」という。）と統一感がない。	御意見として参考にさせていただきます。
224	その他・全般	システム運用編 （Control）	【はじめに】	P1	「医療情報システムの形態に応じた」の解釈として、医療機関が採用している情報システムが複数ある場合には、そのそれぞれの情報システムの形態に応じた箇所を参照すればよい（医療機関ごとではなく、システムごとに参照箇所が異なる）という理解でよいか、適用関係を明瞭化いただきたい。	システムの全体の構成等により参照パターンが異なるため、複数の情報システムを導入している等の場合にあっては、必要に応じて、システムの提供元である事業者に参照パターンを確認してください。
225	その他・全般	企画管理編 （Management）	目次	i ～ v	他編と同様に目次から目的のページへ移動できるようにして欲しい。	御意見として参考にさせていただきます。
226	その他・全般	企画管理編 （Management）	１０．運用に対する点検・監査	P39	３章【遵守事項】⑧ですでに体制を整備することを要求しているので、ここでは端的に実施に対する要求を明記し、さらに１０．２で解説している「内部監査」、「外部監査」があることから、【遵守事項】④は下記の通りに修正してはどうか。 （変更案）医療情報システムの安全管理に対する内部監査及び外部監査を定期的に実施すること。	御意見として参考にさせていただきます。

227	その他・全般	システム運用編（Control）	４．リスクアセスメントを踏まえた安全管理対策の設計	P10	【遵守事項】②の「例えば、」以降は、後述に解説で説明されているのでここで例示する必要は無く記載不要。	御意見として参考にさせていただきます。
228	その他・全般	すべて	－	－	市からの健診業務（市民健診・がん検診）などの患者情報についての扱いとして、実施主体の市、実施医療機関、画像を管理する業者もこのガイドラインに扱う対象範囲内でしょうか。それぞれ経営者、企画管理、システム運用者の何処に落とし込んだら良いでしょうか。	自治体が実施する健診については、実施医療機関が「医療機関等」として本ガイドラインの対象となります。
229	その他・全般	システム運用編（Control）	【はじめに】	P1	「委託事業者におかれても」の委託事業者は何を指すのか明記がない。	概説編に定義のある「医療情報システム・サービス事業者」と同義です。
230	その他・全般	システム運用編（Control）	１０．医療情報ステム・サービス事業者による保守対応等に対する安全管理措置	P26	本資料は医療機関等のシステム運用担当者編であるため、【遵守事項】②の対象は「事業者」ではなく「医療機関等」ではないか。	医療機関等が事業者に遵守させるべき事項として記載しているため原案通りとします。
231	その他・全般	他(参考資料)	Ｑ＆Ａ （案）	－	目次を作成いただきたい。	御指摘を踏まえ目次を作成しました。
232	その他・全般	他(参考資料)	－	－	5.2版にある「付表１ 一般管理における運用管理の実施項目例」のようなBCPの下地になるような資料を用意していただきたい。	今後の検討にあたっての参考とさせていただきます。
233	その他・全般	企画管理編（Management）	１６．５ 運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合	P60	AIなどを活用した高精度OCRも実用化されているため、患者名や薬剤師名で文字検索できると検索性、すなわち利便性があがると思われ、「例えば電子化化した後の利便性のためOCRの活用が望ましい」等の追加があればよいのではないか。	御意見として参考にさせていただきます。
234	その他・全般	システム運用編（Control）	１２．３．１ 記録媒体等の経年変化の管理・委託事業者への配送等	P60	医療機関等が具体的な対応方法としての参考に、可搬媒体の耐久性の経年変化に対応する有益な参考情報として、JIS Z 6017電子化文書の長期保存方法があるため、本文あるいはＱ＆Ａで、「JIS Z 6017を参照すると良い」などの記載を追加していただきたい。	御意見として参考にさせていただきます。
235	その他・全般	他(参考資料)	Ｑ＆Ａ （案） シＱ－66	P103	２パラは「スキャナよりも適切に動画撮影をすることでの電子化が望ましい」との記載に読めるが、 ①これは、撮影された動画ファイルについて、これまでと同様に電子署名法に基づき、電子署名およびタイムスタンプを付すことで真正性を担保するという理解で正しいか。 ②この記載は動画ファイルを原本とするとも読み取れるため、動画の解像度や転送レート、圧縮伸張方式などのガイドラインが必要ではないか。	①「１４．法令で定められた記名・押印のための電子署名」は、診療情報提供書や診断書等の法令で記名・押印することが定められた文書等を対象としています。これら以外の文書等にタイムスタンプを付加することは必須ではありません。 ②御意見として参考にさせていただきます。
236	その他・全般	概説編（Overview）	２．３ 医療情報システムの範囲	P2	なお書きの一文は、医事システムや同一ネットワーク上にある情報システムが対象でないように誤認される恐れがあるため、「なお、医療情報を含まない情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。」と、「患者への費用請求に関する」を削除するべきではないか。	御意見として参考にさせていただきます。なお、医療情報システムの範囲については、Q&A（概Q-5）に記載があります。
237	その他・全般	システム運用編（Control）	【別添】１．「見読性」確保のための対策	P50	（２）見読化手段の管理について第6.0 版での記述箇所として5.1と記載されているが、5.1に記載されているのは、「可用性」の話であり、可用性を満たせば見読性が満たされるように誤解される恐れがあるため、第5.2版で求めていた「電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である機器、ソフトウェア、関連情報等は常に整備された状態にすること。」に関する記載をすることで見読性への対応を明確に記載しておくことが必要ではないか。	見読性については、システム運用編「5.システム設計の見直し」【遵守事項】④に記載があります。
238	その他・全般	すべて	－	－	概説編「４．１．１ 医療情報システムで取り扱う医療情報の重要性」にて医療情報システムで取り扱う医療情報の重要性について又「４．３ 医療情報システムの安全管理に関連する法令」にて医療情報システムに直接関連する法令として、個人情報保護法を挙げているが、医療者の守秘義務は刑法134条（医師・歯科医師・薬剤師・助産師）をはじめ、貴省資料（http://www.mhlw.go.jp/shingi/2004/06/s0623-15p.html）に列挙されている多くの法令で求められていることから以下の修正等をしてはどうか。 ・概説編４．１．１の２行目は「当該情報は、刑法第１３４条及び各医療関係資格法において定められた守秘義務の対象であり、適切な管理がなされなければ、患者の生命、身体の安全に直接影響を及ぼす可能性があるものであるため、慎重な取扱いが求められる。」に改訂。 ・概説編４．３に上記法令を追記或いは別紙として一覧を添付。 ・経営管理編１．１．１：医療者の守秘義務に関する記載として、「患者等との関係において、医療情報を取り扱う医療情報システム」を「患者等との関係において、守秘義務の対象である医療情報を取り扱う医療情報システム」に改訂。 ・企画管理編１．１．２：「さらに、医療従事者等が作成する医療情報を含むデータに対して電子署名を施す必要がある場合には、」から始まる一文は、「e-文書法で電子保存が認められた文書への署名押印については、同法厚生労働省令において、電子署名法で求める電子署名を持って代えることができるとされている。」という根拠に基づく記載箇所と考えられるため、「電子署名法等に従うこと」を「e-文書法及び関連法令等に従うこと」に改訂。	御意見として参考にさせていただきます。
239	その他・全般	経営管理編（Governance）	１．４ 第三者提供における責任	P8	２項目目において第三者提供を行った情報に対する情報提供元の管理責任は、提供完了を持って離れることが記載されているが、提供と直接関わらない記載が書かれていることで理解が困難になっていると思われ、同項「責任は離れるが、」を「責任は離れる。」とし、以降の文を削除もしくは注記扱いでの記載に改訂してはどうか。	ご指摘を踏まえ、提供元の医療機関等に残る医療情報に対する適切な管理責任については、なお書きで記載いたします。

240	その他・全般	経営管理編 （Governance）	３．４．３ 情報セキュリティインシデントへの対応体制	P18	セキュリティインシデント発生時に各所に連絡をする必要があるのであれば、経営管理編に別紙等の形で連絡することが求められている連絡先一覧を提供いただきたい。	今後の検討にあたっての参考とさせていただきます。
241	その他・全般	企画管理編 （Management）	―	P9 P18	大学病院などのように医療機関が法人全体の一部を為す場合には、上位機関である法人等においてセキュリティポリシーやCSIRTが定められ、法人全体の整合性がとられる必要があることがあるため、以下としてはどうか。 ・１．２．１に「医療機関等が所属する法人等において情報セキュリティ方針等が別に定められている場合には、当該医療機関等に特有の事項への該当性等について検討し、必要に応じて附則等を整備すること。」などの追記。 ・３．１．５に 「医療機関等が所属する法人等においてCSIRT等が別に整備されている場合には、当該医療機関等に特有の事項への該当性等について検討し、必要に応じて別途整備することなどを検討すること。」などの追記。	御指摘を踏まえ修正しました
242	その他・全般	企画管理編 （Management）	２．リスク評価を踏まえた管理	P9	医療情報システムの安全管理を運用するためのセキュリティ体制を整えていくための、補助金などを設立して体制整備を支援していくべきである。	今後の検討にあたっての参考とさせていただきます。
243	その他・全般	企画管理編 （Management）	―	―	医療機関単独で対応できずシステム事業者の主導による管理等が想定されていることから、ガイドラインに関する問い合わせ先を明確にするとともに、ガイドラインに記載してほしい。	担当部署については、本ガイドラインを掲載するホームページ内に記載いたします。
244	その他・全般	―	―	―	行政としてベンダ向けのガイドラインの作成と、医療機関へのベンダ認証（ガイドラインに沿った責任分界点への対応、レポート体制、インシデント発生時の対応など）を取り入れるなど、医療機関から相談しやすい体制をベンダ業界側にも構築し、医療機関等のサイバーセキュリティ対策を担うベンダの質が確保できるよう、行政として必要な対策を行うべき。	御意見として参考にさせていただきます。なお、経済産業省及び総務省において、「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」を作成しています。
245	その他・全般	―	―	―	2023年度からは、ガイドライン遵守が求められる対象事業所が圧倒的に広がったことや全ての事業所にセキュリティ対策を習熟した従業者がいるわけではないことから、わかりやすく表現し、医療現場の対応が進みやすくなるよう改善を求める。	御意見として参考にさせていただきます。
246	その他・全般	―	―	―	ガイドラインに沿った運用を行うための質問・相談窓口の設置いただいた上で、「よくあるお問い合わせ」等を公開し情報提供を促進して欲しい。	御意見として参考にさせていただきます。
247	その他・全般	―	―	―	医療法第25条第１項の立入検査のようなチェックする体制よりも、遵守させるための講習会の充実を求める。	御意見として参考にさせていただきます。
248	その他・全般	―	―	―	損害を受けた場合には、医療機関が経営困難とならないよう、施設基準の特例措置や診療報酬等の概算請求を認めるよう求める。	御意見として参考にさせていただきます。
249	その他・全般	―	―	―	医療機関は医療を提供するところであり、政府・行政が医療機関にDXを求めるのであれば、相対的にセキュリティ対策についても補助金及び研修の体制を整えていくべきであり、公的・民間を問わず全ての医療機関等がサイバーセキュリティ対策を講じられるよう補助金を通じて体制整備を支援していくべき。	御意見として参考にさせていただきます。
250	その他・全般	他(参考資料)	―	―	様々な運用規程、指針、契約書、院内研修、管理・記録簿、チェックリスト、機器・システム・サービスの仕様書、患者・利用者又はその家族に対する説明文書などについて、様式または見本（例示）若しくはポイントが欲しい。	御意見として参考にさせていただきます。
251	その他・全般	―	―	―	既存の「匿名加工医療情報」に加え、「仮名加工医療情報」のように利用可能なデータの粒度が改善することが、新たな医学知見の創出や医療AI・SaMD等の産業導出物に、さらには医療データサイエンス・AI開発による今後の医療産業の活性化に繋がると考えていること等から、「医療情報システムの利活用を前提としたデータ取り出し経路の確保」について追記いただきたい。	御意見として参考にさせていただきます。
252	その他・全般	概説編 （Overview）	４．４ 医療情報システムに関する統制	P8	最後の一文は表３－１に示す医療機関等の特性に応じた記載にすべく、以下としてはどうか。 （変更案） 加えて、「３．２．１ 医療機関等の特性についての考え方」で示しているII/IV（いわゆるクラウドサービス型）の該当事業者に対して、必要に応じて、「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」の遵守状況を確認するなど、当該事業者の管理も求められる。 I/III（いわゆるオンプレミス型）の該当事業者に対して、必要に応じて、日本画像医療システム工業会（JIRA）の工業会規格（JESRA：Japanese Engineering Standards of Radiological Apparatus）及び保健医療福祉情報システム工業会（JAHIS）のJAHIS 標準となっている「『製造業者/サービス事業者による医療情報セキュリティ開示書』ガイド」により本ガイドラインの対応状況を確認するなど、当該事業者の管理も求められる。	御意見として参考にさせていただきます。
253	その他・全般	他(参考資料)	Ｑ＆Ａ （案） シＱ－13	P68	「検像の定義」は公益社団法人日本放射線技術学会が公表している「画像情報の確定に関するガイドライン Ver.2.1」に明確に記載されているため参照するように促してはどうか。	ご指摘を踏まえ修正いたします。
254	その他・全般	すべて	―	―	ガイドラインの骨子を経営管理編、企画管理編、システム運用編と分けることで医療機関内の各役割を明確にする狙いがある見受けられるところ、多くの医療現場では、その役割が重複される場合が散見されるため、本ガイドラインで示された「企画管理者」がどのような教育、資格を有することでその役目を担うことができるのか、またはどのような方向性となるのかを実例を明示する形で示していただきたい。また、ネットワークにつながり医療情報システムの一部となっている医療機器の管理、リモート保守について具体的に示していただきたい。	今後の検討にあたっての参考にさせていただきます。なお、医療機関におけるネットワークに接続された医療機器の管理及び医療機器の保守に関する責任・役割等については、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」に記載されています。
255	その他・全般	すべて	―	―	①電子カルテの真正性の確保が不可欠であるとの考えから、すべての電子カルテがデータの改ざんができない仕様のものとなるよう、電子カルテの規格を統一するべき。 ②電子カルテの真正性の確保が不可欠であるとの考えから、電子カルテのデータを開示する際に「履歴あり」や「履歴なし」の仕様があることを国民に周知すべきではないか。 ③電子カルテの真正性の確保が不可欠であるとの考えから、電子カルテの付箋機能を使って、カルテ開示を請求する患者に知られたくない情報を隠す手法等の発想が起こりえないようにガイドライン等で規定すべき。 ④電子カルテの真正性の確保が不可欠であるとの考えから、電子カルテの保存義務を無期限とし、正当な理由なくカルテの情報が消去されることがないようにするべき。 ⑤電子カルテの真正性の確保が不可欠であるとの考えから、患者との情報共有ができるよう、患者が自分の電子カルテの情報にアクセスしやすい便利なシステムとなるよう規定すべき。	電子化された診療情報の真正性の確保のため、ガイドラインのQ&A（シQ-57）では、更新履歴の保存を要件の一つとして記載しています。具体的には、診療行為等に基づく記録の更新と、不正な記録の改ざんは容易に判別されなければならないという観点から、記録の更新内容・更新日時を記録すること及び更新内容の確定を行った確定者の識別情報を関連付けて保存しなければならないとしています。 このように、電子カルテ情報の真正性確保のための最大限の努力を求めた上で、保存年限の撤廃などの御意見については、今後の検討にあたっての参考にさせていただきます。なお、電子カルテ情報の開示については、御意見を踏まえ、適切な対応に関して周知することを検討いたします。