

各編間相関表

経営管理編		企業管理編		システム運用編	
記載箇所	遵守事項	記載箇所	遵守事項	備考	遵守事項
1.1 安全管理に関する法令の遵守	① 医療情報システムの安全管理に開示する法令等を遵守すること。	5.2版のA項に関する前編を対照して新設	① 医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要措置を講じること。		① 法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。
	② 医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関する法令等を遵守させること。	5.2版のA項に関する前編を対照して新設	② 委託先の医療情報システム・サービス事業者等に対して①に関連して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。		
1.2 医療機関等における責任	① 医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。	5.2版第4の趣旨を踏まえて新設	④ 医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程の整備を行い、経営層の承認を取ること。		
	② 患者等への説明を適切に行うための窓口の設置等の対策を行うこと。	5.2版第4の趣旨を踏まえて新設	⑦ 患者等からの問い合わせ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。		
1.3 情報セキュリティインシデントが生じた場合、医療機関等内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。	① 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患者、関係機関等に説明する体制を速やかに構築すること。	5.2版4.1B(2)①の趣旨を踏まえて新設	⑩ 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		
	② 情報セキュリティインシデントが生じた場合、医療機関等内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。	5.2版6.10B(4)の趣旨を踏まえて新設	⑩ 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		

	【事後策を講ずる責任】			12. サイバー攻撃対策	<p>⑥ サイバーセキュリティ事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をおらかじめ整理した上で、必要に応じて契約等を行うこと。(ここの関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。)</p> <p>⑦ 非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、通常、非常時の対応手順等に反映させること。</p>
	⑩ 情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講ずること。	52版4.1B(2)②の趣旨を踏まえて新設	11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		① 医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等遵守し、委託先事業者の選定や管理を適切に行うこと。
1.3 委託における責任	1.3.1 委託（第三者委託）における責任	52版8.3の趣旨を踏まえて新設	1. 管理体制	<p>② 委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じよう契約において定め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。</p> <p>③ 外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。</p> <p>a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況</p> <p>b 医療情報等の安全管理に係る実施体制の整備状況</p> <p>c 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況</p> <p>d 実績等に基づく個人データ安全管理に関する信用度</p> <p>e 財務諸表等に基づく経営の健全性</p> <p>f プライバシーマーク認定又はISMS 認証の取得</p> <p>g 「医療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</p> <p>・政府情報システムのためのセキュリティ評価制度 (ISMIP)</p> <p>・JASA クラウドセキュリティ推進協議会CSゴールドマーク</p> <p>・米田 FedRAMP</p> <p>・AICPA SOC2 (日本公認会計士協会 IT7 号)</p> <p>・AICPA SOC3 (SysTrust/WebTrust) (日本公認会計士協会 IT2 号)</p> <p>上記認証等が確認できない場合、下記のとおりそれぞれの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること</p> <p>・システム監査技術者</p> <p>・Certified Information Systems Auditor ISACA 認定</p> <p>h 医療情報を保存する情報機器が設置されている場所(地域、国)</p> <p>i 委託先事業者に対する国外法の適用可能性</p>	<p>⑤ 外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。</p> <p>－ 保存した医療情報の取扱いに関して監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に関連した場合のペナルティを契約等で定めること。</p> <p>－ 医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。</p> <p>－ 総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。</p> <p>－ 外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。(例えば、「医療情報を取り扱うシステム・サービスの提供事業者における安全管理ガイドライン」における「サービス継続適合性」の提供を求め確認することなどが挙げられる。)</p> <p>－ 外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。</p> <p>－ 保存した情報 (Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。) を診断・分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。</p> <p>－ 保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な制限を設定させ、情報漏洩や、誤った開示 (異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等) が起こらないよう求めること。</p> <p>－ 保存された情報を格納する情報機器等が、国内法の適用を受けられることを確認すること。</p>
1.3.2 委託（第三者委託）における責任	① 業務等を委託する場合は、委託する業務等の内容及び責任範囲並びに役割分担等の責任分界を明確にし、認識の齟齬が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。	6.11C6 10C1(7)	7. 安全管理のための人的管理 (従業者管理、委託先管理、教育・訓練、委託先選定・契約)	<p>⑦ 安全管理のための人的管理 (従業者管理、委託先管理、教育・訓練、委託先選定・契約)</p> <p>⑧ 委託先事業者が契約に基づいて必要の対応を行っていることを定期的に確認するため、委託先事業者に報告を求め、当該報告の結果、改善が必要である場合にはその旨を確認すること。また委託先事業者からの報告内容については、経理層に報告し、承認を得ること。</p> <p>⑨ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。</p>	<p>⑦ 医療情報の外部保存の委託先事業者との契約には、以下の内容を定めること。</p> <p>－ 委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。</p> <p>－ 保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。</p> <p>－ 匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。</p> <p>－ 保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるように仕組みを提供する場合は、外部保存の委託先事業者に適切な利用制限や開示の制限を設定し、情報漏洩や、誤った開示 (異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等) が起こらないよう配慮すること。</p> <p>－ 情報の提供は、原則、患者が受診している医療機関等と患者との間で同意に基づいて実施すること。</p>
1.4 第三者提供における責任	① 医療情報を第三者提供する場合、法令等遵守し、手続き等の記録等を適切に管理する体制を整備すること。	52版4.2.2の趣旨を踏まえて新設	1. 管理体制	<p>① 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>② 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>③ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>④ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑤ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑥ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>	<p>③ 委託先事業者が契約に基づいて必要の対応を行っていることを定期的に確認するため、委託先事業者に報告を求め、当該報告の結果、改善が必要である場合にはその旨を確認すること。また委託先事業者からの報告内容については、経理層に報告し、承認を得ること。</p> <p>④ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。</p> <p>⑤ 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。</p> <p>⑥ 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>⑦ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>⑧ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>⑨ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑩ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑪ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>
2.1 医療情報システムにおけるリスク評価の実施	① 取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	6.2C4	2. 責任分界	<p>① 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>② 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>③ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>④ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑤ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑥ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>	<p>③ 委託先事業者が契約に基づいて必要の対応を行っていることを定期的に確認するため、委託先事業者に報告を求め、当該報告の結果、改善が必要である場合にはその旨を確認すること。また委託先事業者からの報告内容については、経理層に報告し、承認を得ること。</p> <p>④ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。</p> <p>⑤ 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。</p> <p>⑥ 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>⑦ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>⑧ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>⑨ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑩ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑪ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>
2. リスク評価を踏まえた管理	① 取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	6.2C4	6. リスクマネジメント	<p>① 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>② 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>③ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>④ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑤ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑥ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>	<p>③ 委託先事業者が契約に基づいて必要の対応を行っていることを定期的に確認するため、委託先事業者に報告を求め、当該報告の結果、改善が必要である場合にはその旨を確認すること。また委託先事業者からの報告内容については、経理層に報告し、承認を得ること。</p> <p>④ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。</p> <p>⑤ 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。</p> <p>⑥ 医療情報システム等の安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要の対応を行うこと。</p> <p>⑦ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。</p> <p>⑧ 医療情報システム内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講ずること。</p> <p>⑨ 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。</p> <p>⑩ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。</p> <p>⑪ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。</p>

① システム運用

② システム運用

③ システム運用

④ システム運用

⑤ システム運用

⑥ システム運用

⑦ システム運用

⑧ システム運用

⑨ システム運用

⑩ システム運用

⑪ システム運用

⑫ システム運用

⑬ システム運用

⑭ システム運用

⑮ システム運用

⑯ システム運用

⑰ システム運用

					<p>11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定</p>		<p>② 医療機関等が定める非常時の定義やBCP（Business Continuity Plan：事業継続計画）との整合性を確認して対応方針を策定すること。</p>									
	<p>③ 経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。</p>	6.2C4		<p>リスク分析を踏まえた対応について新設</p>	6. リスクマネジメント		<p>⑥ 経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。</p>					<p>4. リスクアセスメントを踏まえた安全対策の設計</p>	<p>① 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講ずること。</p>			
	<p>2. 2. 1 リスク評価を踏まえたリスク管理</p>	<p>① リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。</p>	6.2C4	<p>リスク分析を踏まえた対応について新設</p>	6. リスクマネジメント		<p>⑧ リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて各安全管理対策を講ずること。</p>					<p>4. リスクアセスメントを踏まえた安全対策の設計</p>	<p>② 事業者から技術的対策等の情報を収集すること。例えば、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」における「サービ仕接続合則示書」を利用することが考えられる。</p>			
	<p>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）の取組</p>	<p>① リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMSを策定し、実施すること。</p>	6.2C4	<p>リスク分析を踏まえた対応について新設</p>	6. リスクマネジメント	<p>⑦ リスク評価の結果、リスク管理の方針に関する説明責任に関する資料を整理し、経営層が説明責任を果たすために必要対応を行うこと。</p>	<p>⑨ PDCAモデルに基づくISMS（Information Security Management System：情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMSが適切に実施されていることを確認し、経営層にその状況を報告すること。</p>					<p>4. リスクアセスメントを踏まえた安全対策の設計</p>	<p>③ 事業者から技術的対策等の情報を収集すること。例えば、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」における「サービ仕接続合則示書」を利用することが考えられる。</p>			
	<p>2. 2. 3 リスク分析を踏まえた要務仕絡適合性の管理</p>	<p>① 医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要務仕絡への適合性を確認し、管理すること。</p>	6.2.3C4	-	6. リスクマネジメント		<p>⑩ リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて各安全管理対策を講ずること。</p>					<p>4. リスクアセスメントを踏まえた安全対策の設計</p>				
	<p>3. 1. 1 情報セキュリティ対策のための統制</p>	<p>① 統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を確保するために必要な規程類、管理体制等を整理するとともに、適切に統制が機能しているかを確認すること。</p>	6.3CS10章	<p>統制についての記述は新設</p>	1. 管理体制	<p>① 管理体制</p>	<p>⑪ PDCAモデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。</p> <p>⑫ 医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求め、その結果を反映すること。</p> <p>⑬ 組織における情報セキュリティ方針、医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し、経営層の承認を得ること。</p> <p>⑭ ⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に適用されているか確認すること。</p> <p>⑮ ①～④までの対応においては、整備した内容を可視化できるようにすること。</p>	<p>① 医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を得ること。</p> <p>② 規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規程類の整備を行うこと。規程類は必要に応じて見直しを行うこと。</p> <p>③ 医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。</p> <p>④ 非常時における医療情報システムの運用に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を統制の上、経営層に報告すること。</p>								
	<p>3. 1. 2 医療情報システムにおける統制上の留意点</p>	<p>① 医療機関等の規程や組織構成、特性等を踏まえた統制の内容を確認し、付表</p>	6.3C1	-	3. 医療機関等における安全管理のための体制と責任・権限	<p>① 医療情報システムの安全管理の責任を担う者としての位置付け、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。</p>	<p>② 情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規程等を策定し、経営層の承認を得ること。</p> <p>③ 安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。</p>	<p>① 非正常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための役割として情報セキュリティ責任者（CISO）やCSIRTなどの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。</p> <p>② 法律上の対応を含め医療情報の漏洩等が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。</p>	<p>① 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。</p>							
	<p>3. 2 設計</p>	<p>① リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。</p> <p>② 情報セキュリティ対策に基づき、自医療機関等の実態を踏まえて、実施可能な内容で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。</p>	10C1(1)a	-	1. 管理体制	<p>① 管理体制</p>	<p>⑤ 組織における情報セキュリティ方針、医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し、経営層の承認を得ること。</p> <p>⑥ 医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。</p>	<p>⑦ 安全管理のための人的管理（従業員管理、委託先管理、教育・訓練、委託先選定・契約）</p>	<p>① 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。</p>	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>17. 記録のレビュー・システム監査</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>			
	<p>3. 2. 2 情報セキュリティ対策を踏まえた訓練・教育</p>	<p>① 医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、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。</p>	10C1(2)c	-	5. 安全管理におけるエビデンスの考え方	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>				<p>17. 記録のレビュー・システム監査</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>			
	<p>3. 3 安全管理対策の管理</p>	<p>① 医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。</p>	-	<p>①(1)の趣旨を踏まえて新設</p>	3. 医療機関等における安全管理のための体制と責任・権限	<p>③ 収集した証拠に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証拠の整備に関する改善を行うこと。</p> <p>④ 改善で求められる医療情報の管理に関する訓練を、必要に応じて、説明責任を果たせるよう管理すること。</p> <p>⑤ 医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。</p>	<p>③ 収集した証拠に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証拠の整備に関する改善を行うこと。</p> <p>④ 改善で求められる医療情報の管理に関する訓練を、必要に応じて、説明責任を果たせるよう管理すること。</p> <p>⑤ 医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。</p>	<p>③ 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。</p>	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>17. 記録のレビュー・システム監査</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>				
	<p>3. 3 安全管理対策の管理</p>	<p>① 医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、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。</p>	10C1(2)c	-	5. 安全管理におけるエビデンスの考え方	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>③ 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。</p>	<p>① 医療情報システムの安全管理の状況を確認するために必要な証拠について整理し、当該証拠の整備について必要対応を行うこと。</p>	<p>17. 記録のレビュー・システム監査</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>	<p>① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日志等により操作者、操作内容等を記録すること。</p> <p>② アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。</p> <p>③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を確保する必要がある。</p>				

3、4、2 情報共有・支援、情報収集	11、非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		② 医療機関等が定める非常時の定義やBCP（Business Continuity Plan：事業継続計画）との整合性を確認して対応方針を策定すること。			
3、4、2 情報共有・支援、情報収集	11、非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		② 医療機関等が定める非常時の定義やBCP（Business Continuity Plan：事業継続計画）との整合性を確認して対応方針を策定すること。	11、システム運用管理（通常時・非常時等）	① 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。 「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。 「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こと」も、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。 「非常時ユーザアカウントが使用された場合、正常復旧後は継続使用ができないように変更すること」。 「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、関係先への連絡手段や紙での運用等の代替手段を準備すること」。 「サイバー攻撃による被害拡大の防止の観点から、論理的・物理的に構成分離されたネットワークを整備すること」。 「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、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること」。	
3、4、2 情報共有・支援、情報収集	12、サイバー攻撃対策	6.2.3C5の題旨から新設	② サイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、経営層に報告し、承認を得ること。	18、外部からの攻撃に対する安全管理措置	① 医療情報システムに対する不正ソフトウェア混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。 「攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時遮断」 「他の情報機器への混入拡大の防止や情報漏洩の抑制のための当該混入機器の隔離」 「他の情報機器への波及の調査等被害の確認のための業務システムの停止」 「バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、暗号化がサーバ設置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）」。	
3、4、2 情報共有・支援、情報収集	12、サイバー攻撃対策	6.2.3C5の題旨から新設	③ サイバーセキュリティ対応計画を踏まえ、その内容を各規程や手順等に反映すること。	11、システム運用管理（通常時・非常時等）	① 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。 「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。 「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こと」も、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。 「非常時ユーザアカウントが使用された場合、正常復旧後は継続使用ができないように変更すること」。 「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、関係先への連絡手段や紙での運用等の代替手段を準備すること」。 「サイバー攻撃による被害拡大の防止の観点から、論理的・物理的に構成分離されたネットワークを整備すること」。 「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、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること」。	
3、4、3 情報セキュリティインシデントへの対応体制	① 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署や所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。	6.10C5	④ 非常時の事業発生への対応等に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。	12、サイバー攻撃対策		
3、4、3 情報セキュリティインシデントへの対応体制	② 情報セキュリティインシデントが発生した場合に、厚生労働省等への報告のほかに、患者等に対する公表・広報を適切に行える体制を、速く構築すること。	6.10C5	⑤ サイバーセキュリティ対策を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また訓練結果を踏まえ、対応計画の検証・見直しも実施し、必要に応じて対応計画等の改定を行うこと。	12、サイバー攻撃対策		
3、4、3 情報セキュリティインシデントへの対応体制	① 医療情報システムの安全管理に必要な対策項目の概要を認識した上で、企画管理者やシステム運用担当者に対して、それぞれの対策項目に該当する具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。	6.7C4	⑥ サイバーセキュリティ事象による非常時対応が生じた場合に情報交換を行う関係者の情報をあらかじめ整理した上で、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）	7、情報の持出し・管理・破壊等	⑨ 破壊に関する規程を踏まえて、把握した情報類別ごとに具体的な破壊の手順を定めること。手順には破壊を行う条件、破壊を行うことができる職員、具体的な破壊方法を定めること。また情報の破壊については、企画管理者に報告すること。 ⑩ 情報処理機器の自壊を発生する場合、必ず専門的な知識を有するものが行うこと。また、破壊終了後、残存し、読み出し可能な医療情報がないことを確認すること。 ⑪ 外部保存を受託する事業者には破壊を委託した場合は、確実に医療情報が破壊されたことを、証拠または事業者の説明により確認すること。	
	8、情報管理（管理、持出し、破壊等）		⑦ サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事実であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029第1号 医政地発1029第3号 医政研発1029第1号 平成30年10月29日）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。	7、情報の持出し・管理・破壊等	⑫ 物理的安全管理措置	
	8、情報管理（管理、持出し、破壊等）		⑧ 非常時の事業発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。	7、情報の持出し・管理・破壊等	⑬ 物理的安全管理措置	
	8、情報管理（管理、持出し、破壊等）		⑩ 医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破壊等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。	7、情報の持出し・管理・破壊等	⑭ リスクアセスメントを踏まえた安全対策の設計	
	8、情報管理（管理、持出し、破壊等）		⑪ 医療機関等において保有する医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。	7、情報の持出し・管理・破壊等	⑮ 医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理に関する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に確認を行う手順を作成する。	
	8、情報管理（管理、持出し、破壊等）		⑫ 医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。	7、情報の持出し・管理・破壊等	⑯ 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	
	8、情報管理（管理、持出し、破壊等）		⑬ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出し情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。	7、情報の持出し・管理・破壊等	⑰ 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	
	8、情報管理（管理、持出し、破壊等）		⑭ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いた持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。	7、情報の持出し・管理・破壊等	⑱ 持ち出した利用者や情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトウェアやフォールバックの導入等により、情報漏洩が情報漏洩、改ざん等の対象にならないような対策を実施すること。	
	7、情報の持出し・管理・破壊等		⑮ 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順を作成し、適用すること。その際、情報類別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。	7、情報の持出し・管理・破壊等	⑲ 持ち出した情報機器等について、公衆無線LANの利用がなされた場合には、利用後に端末の安全性を確認できる手順を策定すること。	
	7、情報の持出し・管理・破壊等		⑯ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出し情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。	7、情報の持出し・管理・破壊等	⑳ 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	
	7、情報の持出し・管理・破壊等		⑰ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いた持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。	7、情報の持出し・管理・破壊等	㉑ 持ち出した利用者や情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトウェアやフォールバックの導入等により、情報漏洩が情報漏洩、改ざん等の対象にならないような対策を実施すること。	
	7、情報の持出し・管理・破壊等		⑱ 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順を作成し、適用すること。その際、情報類別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。	7、情報の持出し・管理・破壊等	㉒ 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	
	7、情報の持出し・管理・破壊等		⑳ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出し情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。	7、情報の持出し・管理・破壊等	㉓ 持ち出した利用者や情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトウェアやフォールバックの導入等により、情報漏洩が情報漏洩、改ざん等の対象にならないような対策を実施すること。	

						④ 医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程にじたものとして、いることが前提となるよう管理すること。資格や権限に関する実態を認識の仕組みにおいて適切に反映できるように、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。				14. 認証・認可に関する安全管理措置			① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。						
										14. 認証・認可に関する安全管理措置			④ アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるように、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。						
		13. 医療情報システムの利用者に関する認証等及び権限								14. 認証・認可に関する安全管理措置			① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。						
										14. 認証・認可に関する安全管理措置			④ アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるように、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。						
										14. 認証・認可に関する安全管理措置			① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。						
		13. 医療情報システムの利用者に関する認証等及び権限					⑥ 医療情報システムの管理権限や、医療情報システム、情報機器等で用いるID等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて利用される管理権限の種類とそのID、利用が認められている者等を管理して一元化するよう指示すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。			14. 認証・認可に関する安全管理措置				① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。					
										14. 認証・認可に関する安全管理措置			⑦ 医療情報システムにおいて用いるIDについて、台帳管理等を行うほか、定期的に権限を行い、不要なものは適宜削除すること等を含む手順を作成すること。						
		13. 医療情報システムの利用者に関する認証等及び権限					⑦ 医療情報システムで利用するID等についての権限を定期的に行い、不要なものについては削除すること。権限については、担当者に具体的な手順等の策定を指示すること。また、権限結果を経営層に報告し、承認を得ること。			14. 認証・認可に関する安全管理措置				① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。					
										14. 認証・認可に関する安全管理措置			⑦ 医療情報システムにおいて用いるIDについて、台帳管理等を行うほか、定期的に権限を行い、不要なものは適宜削除すること等を含む手順を作成すること。						
		13. 医療情報システムの利用者に関する認証等及び権限					⑧ 電子カルタにおける記録の確定に関して、以下の事項を規程等に含めること。 入力者及び確定者の識別・認証 - 記録の確定手順、識別情報の記録の保存 - 更新履歴の保存 - 代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者			14. 認証・認可に関する安全管理措置				① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。					
										14. 認証・認可に関する安全管理措置			⑦ 医療情報システムにおいて用いるIDについて、台帳管理等を行うほか、定期的に権限を行い、不要なものは適宜削除すること等を含む手順を作成すること。						
										14. 認証・認可に関する安全管理措置			① 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・認証を行い、利用者認証方法に関する手順等に関して、規程、マニュアル等で文書化すること。						
										14. 認証・認可に関する安全管理措置			⑦ 医療情報システムにおいて用いるIDについて、台帳管理等を行うほか、定期的に権限を行い、不要なものは適宜削除すること等を含む手順を作成すること。						
		14. 法令で定められた記名・押印のための電子署名					① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。 1.以下の電子証明書を用いて電子署名を施すこと (1)「電子署名及び認証業務に関する法律」(平成12年法律第102号)第2条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。 (2)法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)→(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名を用いること。【以下略】 2.法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること (1)タイムスタンプは、第三者による検証を可能にするため、「時系列認証業務の認定に関する規程」に基づき認定された事業者(認定事業者)が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者(タイムビジネスに係る指針等で示されている時刻認証事業者の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者、以下「認定時刻認証事業者」という。)については、令和4年度、国による認定制度に順次移行する予定であることから、当分の間、認定時刻認証事業者によるものを使用しても差し支えない。 (2)法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。 (3)タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。 (4)タイムスタンプを付与する時点で有効な電子証明書を用いること。			15. 電子署名、タイムスタンプ			① 法令で定められた記名・押印のための電子署名について、企画管理編「14. 法令で定められた記名・押印のための電子署名」に示す条件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講ずること。						
		14. 法令で定められた記名・押印のための電子署名					② 電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」(CP)等で定める鍵の管理の要件を満たして行われよう、利用者に指示し、管理すること。												
		15. 技術的な対策の管理					① 物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を担当者で実施し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関内において医療情報システムに関する整備計画等を策定している場合には、これを整合性をとること。			12. 物理的安全管理措置				① 医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害(地震、水害、落雷、火災等並びにそれに伴う停電等)に耐えうる機能・構造を備え、災害による障害(結露等)について対策が講じられている建築物に設置することなどを考慮すること。					
		15. 技術的な対策の管理					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(施設、調剤、記録)を行うよう、管理内容を含む規程等を策定すること。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同様である。			12. 物理的安全管理措置				② 医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退室管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入検知装置等を設置されていることを確認すること。					
		15. 技術的な対策の管理					③ 記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。			12. 物理的安全管理措置				③ 個人情報保管されている情報機器等の重要な情報機器には盗難防止を講ずること。					
		15. 技術的な対策の管理					④ 医療情報システムが情報を保存する場所(内部、可搬媒体)を明示し、その場所ごとの保存可能容量(サイズ)、期間、リスク・レスポンス、バックアップの頻度や方法を明確にすること。これらを運用管理規程に定め、その運用を関係者全員に周知徹底すること。			11. システム運用管理(通常時・非常時等)				① 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。 - 「非常時のユーザアカウントや非常時機能」の手順を整備すること。 - 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ことにも、も使用された場合に使用されたことが検知できるように、適切に管理及び監視すること。 - 非常時ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。 - 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、関係先への連絡手段や紙での運用等の代替手段を準備すること。 - サイバー攻撃による被害拡大の防止の観点から、論理的・物理的に構成分離されたネットワークを整備すること。 - 重要なファイルは複数バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。					
										12. 物理的安全管理措置			④ 医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるように、適切に管理すること。						

4. 安全管理に必要な対策全般

4. 1 必要な対策項目の概要

										18. 外部からの攻撃に対する安全管理措置	① 医療情報システムに対する不正ソフトウェア混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。 ・ 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時遮断 ・ 他の情報機器への混入拡大の防止や情報漏洩の抑制のための当該混入機器の隔離 ・ 他の情報機器への波及の調査等被害の確認のための業務システムの停止 ・ バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ設置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）							
										12. 物理的安全管理措置	⑤ 記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の複製を講ずること。							
										8. 利用機器・サービスに対する安全管理措置	③ ソフトウェア構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること、適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。							
										8. 利用機器・サービスに対する安全管理措置	⑧ 常時不正ソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばバターンファイルの更新の確認・維持）を行うこと。							
										8. 利用機器・サービスに対する安全管理措置	③ 医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。							
										8. 利用機器・サービスに対する安全管理措置	④ メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等やむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。							
										8. 利用機器・サービスに対する安全管理措置	⑤ 情報機器に対して起動パスワード等を設定すること。設定にあたっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に依りて必要があれば、定期的なパスワードの変更等の対策を実施すること。							
										8. 利用機器・サービスに対する安全管理措置	⑥ IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。 (1) IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) IoT機器には、製造出荷後にソフトウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。 (3) 使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。							
										18. 外部からの攻撃に対する安全管理措置	① 医療情報システムに対する不正ソフトウェア混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。 ・ 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時遮断 ・ 他の情報機器への混入拡大の防止や情報漏洩の抑制のための当該混入機器の隔離 ・ 他の情報機器への波及の調査等被害の確認のための業務システムの停止 ・ バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ設置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）							
										13. ネットワークに関する安全管理措置 【遵守事項】	① ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。							
										13. ネットワークに関する安全管理措置 【遵守事項】	② 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。							
										13. ネットワークに関する安全管理措置 【遵守事項】	③ オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。							
										13. ネットワークに関する安全管理措置 【遵守事項】	④ オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、eberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に突破されない方法が望ましい。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑤ ルータ等のネットワーク機器において、安全性が確認できず脆弱性を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特にVPN接続による場合は、施設内のルータを経由して見なされる施設間を結ぶ通信経路の間で送受信できないように経路を設定すること。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑥ 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以上に限定した上で、クライアント証明書を利用したTLSクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNを利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsec又はTLS1.2以上により接続する場合、セッション間の回り込み（正規のルートではないクロスセッションへのアクセス）等による攻撃への適切な対策を実施すること。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑦ 利用するネットワークの安全性を確保して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑧ 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。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑨ 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。							
										13. ネットワークに関する安全管理措置 【遵守事項】	⑩ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。							

⑦ 医療機関等において利用するネットワークについて、リスク評価を踏まえつつその認定を担当者と協議して検討し、その結果を経営層に報告の上、承認を得ること。なお、認定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を承認の上、経営層に報告し、承認を得ること。

									13. ネットワークに関する安全管理措置【遵守事項】			① 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。
									13. ネットワークに関する安全管理措置【遵守事項】			② 医療機関等がネットワークを通じて通信を行う際に、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行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。
									13. ネットワークに関する安全管理措置【遵守事項】			③ 医療情報システムにおいて無線LANを利用する場合、次に掲げる対策を実施すること。 ④ 適切な利用以外に無線LANを利用されないようにすること。例えば、ANY接続拒否等の対策を実施すること。 ⑤ 不正アクセス対策を実施すること。例えばMACアドレスによるアクセス制限を実施すること。 ⑥ 不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP等により通信を暗号化すること。 ⑦ 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。
									18. 外部からの攻撃に対する安全管理措置			⑧ 医療情報システムに対する不正ソフトウェア混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。 ⑨ 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時遮断 ⑩ 他の情報機器への混入拡大の防止や情報漏洩の抑制のための当該混入機器の隔離 ⑪ 他の情報機器への波及の調査等被害の軽減のための業務システムの停止バックアップからの重要なファイルの復元(重要なファイルは数世代バックアップを複数の方で(追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ環境やネットワークから切り離したバックアップデータの保管等)で確保することが重要である)
		15. 技術的な対策の管理						⑫ 保守に関する安全管理対策として必要な項目を担当者と協議して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約やSLA等により管理項目について取決めを行うこと。	7. 情報の持出し・管理・破壊等			⑫ 保守業務を行う事業者に対して、原則として個人情報を含むデータの持出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て行うこと。
									7. 情報の持出し・管理・破壊等			⑬ 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。
									8. 利用機器・サービスに対する安全管理措置			⑭ メールやファイル交換にあたっては、実行プログラム(マクロ等含む)が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等やむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。
									9. ソフトウェア・サービスに対する要求事項			⑮ 情報機器、ソフトウェアの改訂履歴、その導入の際に実施が行われた作業の妥当性を検証するためのプロセスを規定すること。
									10. 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			⑯ 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めるとともに、
									10. 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			⑰ 診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。
									10. 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			⑱ 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。なお、これは利用者を通じて操作確認を行う際の識別・認証についても同様である。
									10. 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			⑲ リモートメンテナンス(保守)によるシステムの改訂・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めるとともに、
									10. 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			⑳ リモートメンテナンス(保守)において、やむを得ず事業者が、ファイルや医療機器等へ送信等を行う場合、送信側で無害化が行われていることを確認すること。
									10. 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			㉑ 診療録等を保管している設備に障害が発生した場合等、やむを得ず診療録等にアクセスする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。
		15. 技術的な対策の管理						⑳ 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定めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じたために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。	10. 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			㉒ 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めるとともに、
									10. 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			㉓ 診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。
									10. 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			㉔ 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。なお、これは利用者を通じて操作確認を行う際の識別・認証についても同様である。
		15. 技術的な対策の管理						㉕ 医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協議して検討すること。	9. ソフトウェア・サービスに対する要求事項			㉕ システムがどのような情報機器、ソフトウェアで構成され、どのような場合、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。
									9. ソフトウェア・サービスに対する要求事項			㉖ 医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従って必要な措置を講じ、企画管理者に報告すること。
									9. ソフトウェア・サービスに対する要求事項			㉗ システムがどのような情報機器、ソフトウェアで構成され、どのような場合、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。
									9. ソフトウェア・サービスに対する要求事項			㉘ 医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるよう措置を講じること。
									9. ソフトウェア・サービスに対する要求事項			㉙ システムがどのような情報機器、ソフトウェアで構成され、どのような場合、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。
									9. ソフトウェア・サービスに対する要求事項			㉚ 情報機器、ソフトウェアの改訂履歴、その導入の際に実施が行われた作業の妥当性を検証するためのプロセスを規定すること。
									15. 技術的な対策の管理			㉛ システム更新の際の移行を行えるように、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。
									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)			㉜ システムデータの更新の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。
									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)			㉝ 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。保存義務のある期間中、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。
									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)			㉞ 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。また、見直し手段である情報機器、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。
									9. ソフトウェア・サービスに対する要求事項			㉟ 医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるよう措置を講じること。

