各編間相関表

経営管理編					企画管理編						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	記載箇所			遵守事項			備考
1．安全管理に関する責任・責務	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関係する法令等を遵守すること。	–	5.2版のA項に関する前提を対策として新設														
			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係する法令等を遵守させること。	–	5.2版のA項に関する前提を対策として新設	1．管理体系			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、必要な措置を講じること。				1．情報セキュリティの基本的な考え方			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。	10C2-4		
						1．管理体系			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も①に関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．管理体系			③ 医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認を取ること。また、遵守状況に応じて必要な改善措置を講じること。										
						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			③ 非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。										
						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）～（e）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等を用いること。【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、「時刻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業務の基準に準拠し、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年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。 (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。												
	1.2 医療機関等における責任	通常時における責任																	
		【説明責任】	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．医療情報の安全管理において必要な規程・文書類の整備			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、経営層の承認を取ること。										
						4．医療情報の安全管理において必要な規程・文書類の整備			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則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。										
						4．医療情報の安全管理において必要な規程・文書類の整備			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。				2．システム設計・運用に必要な規程類と文書体系			③ 医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。	10C1-4		
													2．システム設計・運用に必要な規程類と文書体系			④ 医療情報システムの利用者が適切に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。	10C1		
						4．医療情報の安全管理において必要な規程・文書類の整備			④ 非常時における医療情報システムの運用等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、整備状況を確認の上、経営層に報告すること。				2．システム設計・運用に必要な規程類と文書体系			① 医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。	6.2C4 6.9C5		
													2．システム設計・運用に必要な規程類と文書体系			② 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態を維持すること。	6.2C4		
			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	1．管理体系			⑦ 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。										
						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			⑨ 患者等からの相談や苦情への対応を行うための体制を構築すること。										
						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）			⑩ 外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。										
						8．情報管理（管理、持出し、破棄等）			⑨ 患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。										
		【管理責任】	① 医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。	6.3C1-5 第10章	–	1．管理体系			① 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て、その結果を反映すること。										
			② 定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。	6.3C1-5 第10章	–	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			⑧ 医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。										
		【定期的に見直し必要に応じて改善を行う責任】	① 医療情報システムに関する安全管理を適切に維持するための計画を策定すること。	–	5.2版第5章の趣旨を踏まえて新設	10．運用に対する点検・監査			④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。										
						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。										
						12．サイバー攻撃対策			⑤ 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は、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。										
			② 医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。	–	5.2版6.2の趣旨を踏まえて新設	4．医療情報の安全管理において必要な規程・文書類の整備			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則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。										
						10．運用に対する点検・監査			④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。										
						12．サイバー攻撃対策			⑤ 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は、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。										
						15．技術的な対策の管理			⑥ システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。										
		1．2．2 非常時における責任																	
		【説明責任】	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。	6.10C5	5.2版4.1B(2)①の趣旨を加味	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			⑧ 非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。										
						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			⑨ 非常時の事象が生じた場合、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。										
						12．サイバー攻撃対策			① サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。										
						12．サイバー攻撃対策			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またはそのおそれがある事案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。										
			① 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	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			⑧ 非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。										
						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			⑩ 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、適宜、非常時の対応手順等に反映させること。										

		【善後策を講ずる責任】				12．サイバー攻撃対策			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。）											
			②　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じること。	–	5.2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			⑨　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、適宜、非常時の対応手順等に反映させること。											
		1.3.2　委託（第三者委託）における責任分界	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、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。	–	5.2版8.3の趣旨を踏まえて新設	1．管理体系			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。											
						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）			⑥　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。 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 b　医療情報等の安全管理に係る実施体制の整備状況 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 d　実績等に基づく個人データ安全管理に関する信用度 e　財務諸表等に基づく経営の健全性 f　プライバシーマーク認定又はISMS 認証の取得 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 ・政府情報システムのためのセキュリティ評価制度（ISMAP） ・JASA クラウドセキュリティ推進協議会CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7 号） ・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果 により、上記と同等の能力の有無を確認すること ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 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) i　委託先事業者に対する国外法の適用可能性											
	1.3.1　委託（第三者委託）における責任					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）			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。 －　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違反した場合のペナルティを契約書等で定めること。 －　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。 －　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。 －　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「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。） －　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。 －　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。）を勝手で分析、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。 －　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、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。 －　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ることを確認すること。											
						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）			⑦　医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。 －　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。 －　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。 －　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。 －　保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。 －　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の同意に基づいて実施すること。											
						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）			⑧　委託先事業者が契約に基づいて必要な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ること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。											
						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）			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。											
		1.3.2　委託（第三者委託）における責任分界	①　業務等を委託する場合には、委託する業務等の内容及び責任範囲及びに役割分担等の責任分界を明確にし、認識の齟齬等が生じないよう、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)	5.2版4.2の趣旨を加味	1．管理体系			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。											
	1.4　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、法令等を遵守し、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。	–	5.2版4.2.2の趣旨を踏まえて新設	2．責任分界			①　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。											
						5．安全管理におけるエビデンスの考え方			①　医療情報システム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な対応を行うこと。											
			②　医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。	–	5.2版4.2.2の趣旨を踏まえて新設	2．責任分界			④　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。				3．責任分界		⑤　第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。		6．安全管理を実現するための技術的対策の体系	①　システム運用管	
2．リスク評価を踏まえた管理	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	リスク分析を踏まえた対応について新設	6．リスクマネジメント			①　医療機関等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じること。											
			②　リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			②　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。											
						6．リスクマネジメント			③　医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。				4．リスクアセスメントを踏まえた安全対策の設計		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じること。				
						6．リスクマネジメント			④　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。											
						6．リスクマネジメント			⑤　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。				4．リスクアセスメントを踏まえた安全対策の設計		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じること。				
						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関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含めること。				2．システム設計・運用に必要な規程類と文書体系		③　非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。				
													11．システム運用管理（通常時・非常時）		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とともに、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。 － 非常時用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／物理的に構成分割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。				

						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　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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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。										
					6．リスクマネジメント			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じること。			4．リスクアセスメントを踏まえた安全対策の設計			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じること。			
											4．リスクアセスメントを踏まえた安全対策の設計			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「サービス仕様適合開示書」を利用することが考えられる。			
2.2リスク評価を踏まえた判断	2．2．1　リスク評価を踏まえたリスク管理	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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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じること。			4．リスクアセスメントを踏まえた安全対策の設計			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じること。			
											4．リスクアセスメントを踏まえた安全対策の設計			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「サービス仕様適合開示書」を利用することが考えられる。			
		②　リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。										
	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	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。	－	5.2節(6.2.1の趣旨を踏まえて新設	6．リスクマネジメント			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。										
	2．2．3　リスク分析を踏まえた要求仕様適合性の管理	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、医療機関等の要求仕様への適合性を確認し、管理すること。	6.2.3C4	－	6．リスクマネジメント			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じること。										
					6．リスクマネジメント			⑩　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。										
3.1.統制	3．1．1　情報セキュリティ対策のための統制	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、管理体制等を整備するとともに、適切に統制が機能されているかを確認すること。	6.3C5 第10章	統制についての記述は新設	1．管理体系			④　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て、その結果を反映すること。										
					1．管理体系			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。										
					1．管理体系			⑥　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運用されているか確認すること。										
					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			⑩　①～⑨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。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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、経営層の承認を取ること。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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。										
					4．医療情報の安全管理において必要な規程・文書類の整備			④　非常時における医療情報システムの運用等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、整備状況を確認の上、経営層に報告すること。										
	3．1．2　医療情報システムにおける統制上の留意点	①　医療機関等の規模や組織構成、特性等を踏まえた統制の内容を検討すること。	6.3C1 付表	－														
		②　医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。	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			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。										
					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			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。										
					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			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。										
					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			④　非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体制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。										
					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			⑤　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。										
		③　情報セキュリティ対策に関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。	－	統制の趣旨を踏まえ新設														
		④　情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。	－	統制と6.6の趣旨を踏まえ新設	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）			②　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。										
3．2　設計	3．2．1　情報セキュリティ方針を踏まえた情報セキュリティ対策の整備	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。	10C1(1)a	－	1．管理体系			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。										
		②　情報セキュリティ方針に基づき、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。	－	6.3の趣旨を踏まえ新設	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）			①　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。										
	3．2．2　情報セキュリティ対策を踏まえた訓練・教育	①　整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。	6.6C1(2) 6.10C2	－	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			⑥　医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。										
					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）			②　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。										
3．3　安全管理対策の管理	3．3．1　安全管理状況の自己点検	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。	１０C1(2)c	－	5．安全管理におけるエビデンスの考え方			①　医療情報システム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な対応を行うこと。			１７．証跡のレビュー・システム監査			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、業務日誌等により操作者、操作内容等を記録すること。			
											１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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保つ必要がある。			
					5．安全管理におけるエビデンスの考え方			②　証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改ざん等を防止する措置を講じること。			１７．証跡のレビュー・システム監査			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、業務日誌等により操作者、操作内容等を記録すること。			
											１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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保つ必要がある。			
					5．安全管理におけるエビデンスの考え方			③　収集した証跡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、必要があれば証跡の整備に関する改善を行うこと。										
					5．安全管理におけるエビデンスの考え方			④　法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。										
					8．情報管理（管理、持出し、破棄等）			⑩　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。										
		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。	－	4.1(1)の趣旨を踏まえて新設	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			⑧　医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。										

						10．運用に対する点検・監査		①　医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「5．安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。										
		３．３．２　情報セキュリティ監査				10．運用に対する点検・監査		②　医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム・サービスの性格上、報告に基づく確認が難しい場合は、SLAに対する評価等の中で確認すること。										
						10．運用に対する点検・監査		③　医療情報システムの取扱いに関する点検結果を、経営層に報告し、承認を得ること。										
						10．運用に対する点検・監査		④　医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。				１７．証跡のレビュー・システム監査			④　監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。			
			②　内部監査又は外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。	－	4.1(1)の趣旨を踏まえて新設	10．運用に対する点検・監査		④　医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。				１７．証跡のレビュー・システム監査			④　監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。			
３．安全管理全般（統制、設計、管理等）			①　情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準や継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP等を整備すること。	6.10C1	－	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		⑧　非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。										
						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		⑨　非常時の事象が生じた場合、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。										
						12．サイバー攻撃対策		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。）										
						12．サイバー攻撃対策		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案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。										
			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。	6.10C2-4	－	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		⑤　非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。				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とともに、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。 － 非常時用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／物理的に構成分割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。			
													１１．システム運用管理（通常時・非常時等）			②　医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。			
		３．４．１　事業継続計画（BCP：Business Continuity Plan）の整備と訓練	③ 通常時に整備していたBCPが、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。	－	6.10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		⑦　非常時への対応状況を定期的に確認し、経営層に報告のうえ、承認を得ること。										
						12．サイバー攻撃対策		④　サイバーセキュリティ対応計画を踏まえ、対応状況を確認する。技術的な対応・措置については担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。				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とともに、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。 －　非常時用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。 －　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。			
													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の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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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）			
													１１．システム運用管理（通常時・非常時等）			②　医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。			
						12．サイバー攻撃対策		⑧　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は、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。										
						12．サイバー攻撃対策		⑨　サイバーセキュリティ事象による非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応とBCP策定」に示す内容を実施すること。										
		３．４　情報セキュリティインシデントへの対策と対応	①　情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。	－	6.10B(4)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関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含めること。				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とともに、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。 － 非常時用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／物理的に構成分割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。			
													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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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）			

					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．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関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含めること。										
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とともに、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。 － 非常時用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／物理的に構成分割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。			
					12．サイバー攻撃対策			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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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．サイバー攻撃対策			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。										
		②　情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策やEOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示すること。		6.2.3C5の趣旨から新設	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			④　非常時の事象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。				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とともに、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。 － 非常時用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／物理的に構成分割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。			
					12．サイバー攻撃対策			⑤　サイバーセキュリティ対応計画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善を行うこと。										
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	－	12．サイバー攻撃対策			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。）										
					12．サイバー攻撃対策			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案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。										
		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、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。	6.10C5	－	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			⑧　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、適宜、非常時の対応手順等に反映させること。										
		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係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。	6-7章	－	８．情報管理（管理、持出し、破棄等）			①　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、破棄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・破棄等			⑨　破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。			
												７．情報の持出し・管理・破棄等			⑩　情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、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。			
												７．情報の持出し・管理・破棄等			⑪　外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑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、破棄等）			②　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・破棄等			①　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・破棄等			②　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許諾すること。			
					８．情報管理（管理、持出し、破棄等）			③　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。				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、自動侵入監視装置等が設置されていることを確認すること。			
												１２．物理的安全管理措置			③　個人情報が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じること。			
					８．情報管理（管理、持出し、破棄等）			④　医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。				４．リスクアセスメントを踏まえた安全対策の設計			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じること。			
												７．情報の持出し・管理・破棄等			⑦　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。併せて定期的に棚卸を行う手順を作成する。			
					８．情報管理（管理、持出し、破棄等）			⑤　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、持ち出す情報、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・破棄等			①　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、破棄等）			⑥　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る持ち出しのほか、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・破棄等			①　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・破棄等			②　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許諾すること。			
												７．情報の持出し・管理・破棄等			③　医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。			
												７．情報の持出し・管理・破棄等			④　持ち出した利用者が情報機器を、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やパーソナルファイアウォールの導入等により、情報端末が情報漏洩、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・破棄等			⑤　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が確認できる手順を策定すること。			

														7．情報の持出し・管理・破棄等			⑥　持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認すること。			
														7．情報の持出し・管理・破棄等			⑦　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。			
														7．情報の持出し・管理・破棄等			⑧　利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。			
					8．情報管理（管理、持出し、破棄等）			⑦　持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。				7．情報の持出し・管理・破棄等			⑨　医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。			
														7．情報の持出し・管理・破棄等			⑩　医療情報を格納する記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。			
					8．情報管理（管理、持出し、破棄等）			⑧　医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。				7．情報の持出し・管理・破棄等			⑦　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。			
														7．情報の持出し・管理・破棄等			⑧　利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。			
														7．情報の持出し・管理・破棄等			⑨　患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け 、ファイアウォール、アクセス監視、通信のTLS 暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤）認証等の対策を実施すること。			
					8．情報管理（管理、持出し、破棄等）			⑪　医療情報の破棄に関する手順等を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。				7．情報の持出し・管理・破棄等			⑤　破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。			
														7．情報の持出し・管理・破棄等			⑩　情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、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。			
														7．情報の持出し・管理・破棄等			⑪　外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑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、破棄等）			⑫　保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業者における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。				7．情報の持出し・管理・破棄等			⑪　外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑または事業者の説明により確認すること。			
					9．医療情報システムに用いる機器等の資産管理			①　医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、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。）											
					9．医療情報システムに用いる機器等の資産管理			②　医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。											
					9．医療情報システムに用いる機器等の資産管理			③　医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。				8．利用機器・サービスに対する安全管理措置			⑦　企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況など併せて確認すること。			
					9．医療情報システムに用いる機器等の資産管理			④　医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況、脆弱性に関する対応状況等）を確認するよう指示し、報告を受け、適宜必要な対応を行うこと。				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、製品出荷後にファーム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。			
					9．医療情報システムに用いる機器等の資産管理			⑤　医療情報システムが利用するサービスに関して、安全管理の観点から。利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。											
					9．医療情報システムに用いる機器等の資産管理			⑥　医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えばBYOD（Bring Your Own Device：個人保有の情報機器）の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規程等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。				8．利用機器・サービスに対する安全管理措置			⑧　BYOD の実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。			
												8．利用機器・サービスに対する安全管理措置			⑨　BYOD であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。			
					9．医療情報システムに用いる機器等の資産管理			⑦　医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。				8．利用機器・サービスに対する安全管理措置			⑦　企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。			
					13．医療情報システムの利用者に関する認証等及び権限			①　リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規程を整備し、管理すること。											
					13．医療情報システムの利用者に関する認証等及び権限			②　医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。				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、規則、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			②　利用者の識別・認証にユーザID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。			
												14．認証・認可に関する安全管理措置			③　利用者の識別・認証にIC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。。			
												14．認証・認可に関する安全管理措置			④　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、新規導入又は更新するに際しては、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策を行うこと。			
												14．認証・認可に関する安全管理措置			⑤　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。 －　利用者のパスワードの失念や、パスワード漏洩のおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。 － 医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載されて等があってはならない）。			
					13．医療情報システムの利用者に関する認証等及び権限			③　医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者のID 等を付与す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、規則、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			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応じたものとっ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知識を認証の仕組みにおいて適切に反映できるよう、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、規則、マニュアル等で文書化すること。			
																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、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			⑤　医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。医療情報システムの利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じてID やアクセス権限を付与すること。その具体的な手順については、担当者に作成を指示すること。				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、規則、マニュアル等で文書化すること。			
																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、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			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覧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、規則、マニュアル等で文書化すること。			
																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、定期的に棚卸を行い、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 等についての棚卸を定期的に行い、不要なものについては削除すること。棚卸については、担当者に具体的な手順等の策定を指示すること。また、棚卸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、規則、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、定期的に棚卸を行い、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　電子カルテ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、規則、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			⑧　電子カルテにおける記録の確定手順の確定と、識別情報の記録について、以下の機能があることを確認すること。 －　電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 a　診療録等の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。 b　「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。 c　「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。 d　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。 e　一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。 f　確定者が何らかの理由で確定操作ができない場合における記録の確定の責任者の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。			
					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等を用いること。【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、「時刻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業務の基準に準拠し、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年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。 (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、関係省資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」に示す要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じること。			
					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るよう、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と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、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。				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。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、自動侵入監視装置等を設置されていることを確認すること。			
												１２．物理的安全管理措置			③　個人情報が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じること。			
					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。										
					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等を明確にすること。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とともに、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。 －非常時用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／物理的に構成分割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。			
												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、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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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）			
					15．技術的な対策の管理		⑤　記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。					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保管措置を講じること。			
					15．技術的な対策の管理		⑥　システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。					８．利用機器・サービスに対する安全管理措置			①　システム構築時、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			②　常時不正な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（例えばパ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、保守等で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。設定に当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応じて必要があれば、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、製品出荷後にファーム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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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）			
					15．技術的な対策の管理		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選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、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、その内容を確認の上、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　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、erberos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、容易に解読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ついて、安全性が確認できる機器を利用し、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異なる施設間を結ぶ通信経路の間で送受信が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は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ーズド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勘案して、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。			

														１３．ネットワークに関する安全管理措置 【遵守事項】			⑪　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】			⑫　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】			⑬ 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。 － 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、ANY接続拒否等の対策を実施すること。 － 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。 － 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。 － 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			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切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止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、端末及びサーバ装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）			
				15．技術的な対策の管理				⑧　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働して検討すること。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・破棄等			②　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許諾すること。			
														７．情報の持出し・管理・破棄等			③　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			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、保守等で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			②　情報機器、ソフトウェアの改訂履歴、その導入の際に実際に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			①　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			②　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			③　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、これは利用者を模し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			④　リモートメンテナンス（保守）によるシステムの改造・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			⑤　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、ファイルを医療機関等へ送信等を行う場合、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。			
														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			⑥　診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスを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			⑨　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。また、やむを得ず医療情報を用いる場合には、漏洩等が生じない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			①　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			②　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			③　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、これは利用者を模し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				⑩　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、担当者と協働して検討すること。						９．ソフトウェア・サービスに対する要求事項			①　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、どのような場面、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			③　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、これに従い必要な措置を講じ、企画管理者に報告すること。			
				15．技術的な対策の管理				⑪　情報機器、ソフトウェアの品質管理に関する対応を運用管理規程で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。						９．ソフトウェア・サービスに対する要求事項			①　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、どのような場面、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			④　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。			
				15．技術的な対策の管理				⑫　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。						９．ソフトウェア・サービスに対する要求事項			①　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、どのような場面、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			②　情報機器、ソフトウェアの改訂履歴、その導入の際に実際に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				⑬　医療情報システムが法令等で求められている要件を満たすよう適切に管理すること。特に「施行通知」、「外部保存通知」などで求める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容等については、担当者に確認の上、必要な検討を行うよう指示すること。						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）			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。			
														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）			②　マスタデータベースの変更の際に、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）			③　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に、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継持すること。			
														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）			④　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			④　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。			

													１４．認証・認可に関する安全管理措置			⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。 － 電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 a 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。 b 「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。 c 「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。 d 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。 e 一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。 f 確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。			
						16. 紙媒体等で作成した医療情報の電子化			① 紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規程等に定めること。				１６.紙媒体等で作成した医療情報の電子化			① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。			
						16. 紙媒体等で作成した医療情報の電子化			② スキャナにより読み取った電子情報と元の文書等から得られる情報と同等であることを担保する情報作成管理者を配置すること。				１６.紙媒体等で作成した医療情報の電子化			① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。			
						16. 紙媒体等で作成した医療情報の電子化			③ 紙媒体で作成した医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りに係る責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規程等に定めること。なお、電子署名については「14.法令で定められた記名・押印のための電子署名」を参照すること。										
						16. 紙媒体等で作成した医療情報の電子化			④ 情報作成管理者に対して、スキャナによる読み取り作業が運用管理規程に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。				１６.紙媒体等で作成した医療情報の電子化			① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。			
						16. 紙媒体等で作成した医療情報の電子化			⑤ 診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うことを運用管理規程等に定めること。										
						16. 紙媒体等で作成した医療情報の電子化			⑥ 過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。 ・ 対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。 ・ 必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。 － 運用管理規程の作成と妥当性の評価方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を確保した委員会等で行うこと（倫理委員会を用いることも可）） － 作業責任者 － 患者等への周知の手段と異議の申立てに対する対応方法 － 相互監視を含む実施体制 － 実施記録の作成と記録項目（次項の監査に耐え得る記録を作成すること） － 事後の監査人と監査項目 － スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法 ・ 事後の監査は、システム監査技術者やCertified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ外部監査人によって実施すること。										
						16. 紙媒体等で作成した医療情報の電子化			⑦ 企画管理者は、紙の調剤済み処方箋をスキャナ等で電子化して保存する場合、以下の措置を講じること。 ・ 紙の調剤済み処方箋の電子化のタイミングに応じて、⑤又は⑥の措置を講じること。 ・「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。				１６.紙媒体等で作成した医療情報の電子化			② 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、以下の措置を講じること。 ・ 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。 ・ 緊急に閲覧が必要になったときに迅速に対応できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。			
						16. 紙媒体等で作成した医療情報の電子化			⑧ 企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。 ・ 情報作成管理者が、スキャナによる読み取り作業が適正な手続で確実に実施される措置を講じる旨を運用管理規程等に定めること。 ・ 電子化した後、元の紙媒体やフィルムの安全管理を行うこと。										
			② 対応ができてない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。	－	6.2.1の趣旨から新設	15. 技術的な対策の管理			⑭ ①～⑬において、担当者が整備した対策について、関連規程等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を把握の上、経営層に報告し承認を得ること。										
	４．２ 必要な措置		① 医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。	6.2.3C7	－	１．管理体系			⑥ 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運用されているか確認すること。										
	5.1 事業者選定		① 委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。	8.3C2	－														
			② 委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001 又はこれと同等の規格の認証を受けているシステム関連事業者を選定するよう指示すること。	8.3C2(9)f	2省ガイドラインとの整合性確保														
			① 委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取扱い等、医療機関等が負う医療情報システムの管理に関して、協働する上で認識の齟齬等が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。	－	4.2の趣旨から新設	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）			③ 医療機関等の事務、運用等を外部の事業者に委託する場合は、委託契約の契約書に守秘・非開示に関する内容を含めること。										
						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）			④ ③の委託契約の際に、当該委託先事業者の就業規則等に①及び②の対応を含めるよう求めること。										
		５．２．１ 契約管理				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）			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。 － 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違反した場合のペナルティを契約書等で定めること。 － 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。 － 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。 － 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「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。） － 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。 － 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。）を独断で分析、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。 － 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、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。 － 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ることを確認すること。				７．情報の持出し・管理・破棄等			⑧ セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。			
	５．２ 事業者管理												７．情報の持出し・管理・破棄等			⑭ 患者等に医療情報を閲覧させる場合、医療情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け 、ファイアウォール、アクセス監視、通信のTLS 暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤）認証等の対策を実施すること。			

5．医療情報システム・サービス事業者との協働						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）		②　医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。 －　委託元の医療機関等、患者等の許可なく保存を委託した医療情報を分析等の目的で取り扱わないこと。 －　保存を委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。 －　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。 －　保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切なアクセス権を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。 －　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の同意に基づいて実施すること。				7．情報の持出し・管理・破棄等			③　セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。			
													7．情報の持出し・管理・破棄等			④　患者等に医療情報を閲覧させる場合、医療情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤）認証等の対策を実施すること。			
						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）		⑧　委託先事業者が契約に基づいて必要な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ること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。										
		5．2．2　体制管理	①　委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。	6.6C2(1)d 10C1(5)b		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		⑦　医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。										
	5.3　責任分界管理		①　システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。	－	4.2.1の題旨から新設	2．責任分界		①　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。										
						2．責任分界		②　取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。				3．責任分界			①　医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）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。			
						2．責任分界		③　責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。				3．責任分界			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、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。			
						2．責任分界		④　委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。				3．責任分界			③　通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、企画管理者に対してその結果を報告すること。			
												3．責任分界			④　サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。			
						2．責任分界		⑤　委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、関与する関係者への管理なども責任分界の取決めに含めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。				3．責任分界			③　通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、企画管理者に対してその結果を報告すること。			
												3．責任分界			④　サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。			