参考資料２－５

第5.2 版→第6.0 版 項目移行対応表（案）

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
			記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無
1. はじめに	―	（略）	レ	1、2.1							
2. 本ガイドラインの読み方	―	（略）	レ	3							
3. 本ガイドラインの対象システム及び対象情報	―	（略）	レ	2.2、2.3、4.7	レ	16					
4. 電子的な医療情報を扱う際の責任のあり方	―	（略）	レ	4.1	レ	1.1～1.4、5.3					
5. 情報の相互運用性と標準化について	―	（略）							レ	5	
6.1. 方針の制定と公表	C.最低限のガイドライン	1. 個人情報保護に関する方針を策定し、公開すること。	レ	4.4	レ	1.1	レ	1．2．2			
		2. 医療情報システムの安全管理に関する方針を策定すること。その方針には、次に掲げる事項を定めること。 ・ 理念（基本方針と管理目的の表明） ・ 医療情報システムで扱う情報の範囲 ・ 情報の取扱いや保存の方法及び期間 ・ 不要・不法なアクセスを防止するための利用者識別の方法 ・ 医療情報システム安全管理責任者 ・ 苦情・質問の窓口	レ	4.4	レ	1.1	レ	1．④			
6.2 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践	B.考え方	（略）	レ	4.2							
6.2.1 ISMS構築の手順	B.考え方	（略）			レ	2.2	レ	6.2			
6.2.2 取扱い情報の把握	B.考え方	（略）					レ	6.1.2			
6.2.3. リスク分析	C.最低限のガイドライン	1. 医療情報システムで扱う情報を全てリストアップすること。	レ	4.5	レ	2.2	レ	6．②			
		2. リストアップした情報を、安全管理上の重要度に応じて分類し、常に最新の状態を維持すること。			レ	2.2	レ	6．②			
		3. リストアップした情報は、医療情報システム安全管理責任者が必要に応じて速やかに確認できる状態で管理すること。			レ	2.2	レ	6．1．2			
		4. リストアップした情報に対してリスク分析を実施すること。脅威に関してはリスク分析に関する解説（別冊）を参照	レ	4.5	レ	2.2	レ	6．⑤			
		5. 医療情報システムベンダ及びサービス事業者から技術的対策等の情報を収集すること。例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省　令和2年8月21日）における「サービス仕様適合開示書」を利用することが考えられる。	レ	4.5	レ	2.2	レ	6．⑥	レ	4②	
		6. 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一覧（設置事業者等含む）を作成し、常に最新の状態を維持すること。例えば、前述の「サービス仕様適合開示書」を利用することが考えられる。	レ	4.5	レ	2.2	レ	6．⑥	レ	2②	
		7. リスク分析により得られたリスクに対して、6.3章～6.12章に示す対策を実施すること。			レ	2.2	レ	6．⑧			
	D.推奨されるガイドライン	1. 上記1から7の結果を系統的に文書化して管理すること。			レ	2.2	レ	6．⑦			
6.3 組織的安全管理対策（体制、運用管理規程）	B.考え方	（略）			レ	3.2					
	C.最低限のガイドライン	1. 医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定すること。ただし、小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。			レ	3.2	レ	3① 3③			
		2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めること。			レ	3.2	レ	8③			
		3. 医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	レ	4.4	レ	3.2	レ	8①			
		4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	レ	4.4	レ	3.2	レ	7⑤			
		5. 運用管理規程等において次の内容を定めること。 ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	レ	4.4	レ	3.2	レ				
6.4 物理的安全対策	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。					レ	8③			
		2. 個人情報を入力・参照できる端末が設置されている区画は、業務時間帯以外は施錠するなど、運用管理規程等に基づき許可された者以外の者が立ち入ることができないようにするための対策を実施すること。ただし、上記の対策と同等レベルの他の対策がある場合はこの限りではない。					レ	15②			
		3. 個人情報が保存されている機器が設置されている区画への入退管理を実施すること。例えば、次に掲げる対策を実施すること。 ・ 入退者に名札等の着用を義務付ける。 ・ 台帳等によって入退者を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。					レ	15②			レ
		4. 個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。					レ	8③	レ	12.3.1	
		5. 個人情報が入力・参照できる端末の覗き見防止対策を実施すること。							レ	1 2 .3.2	
	D.推奨されるガイドライン	1. 情報管理上重要な区画に防犯カメラ、自動侵入監視装置等を設置すること。							レ	12②	レ
6.5 技術的安全対策	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 医療情報システムへのアクセスにおける利用者の識別・認証を行うこと。	レ	4.6	レ	4.1	レ	13①	レ	14①	
		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。	レ	4.6			レ	13②	レ	14②	
		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。							レ	14③	
		4. 利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン等の対策を実施させること。					レ	8③	レ	12.3.2	
		5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	レ	4.4			レ	15⑨	レ	10①	
		6. 利用者の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行うこと。また人事異動等による利用者の担当業務の変更等に合わせて、アクセス権限の変更を行うことを、運用管理規程で定めること。なお、複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことでアクセス管理を実施する必要がある。			レ	4.2	レ	13③	レ	14.2	
		7. 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。			レ	4.2	レ	5③	レ	17①	
		8. 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。	レ	4.4	レ	4.2	レ	5②	レ	17②	
		9. 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。					レ	5①	レ	17③	
		10. 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。					レ	9⑥	レ	8①	
		11. 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。	レ	4.4	レ	4.2	レ	15⑥	レ	8②	
		12. 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付等を行う場合、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。					レ	15⑥	レ	8④	
		13. 令和９年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。					レ	15②	レ	14⑤	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		14. 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。 (1) 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。また、利用者識別にICカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者のパスワードの失念や、パスワード漏えいのおそれなどにより、医療情報システムの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、パスワード漏えい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。 (3) 医療情報システムの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記載される等があってはならない）。 (4) パスワードは以下のいずれかを要件とする。 a. 英数字、記号を混在させた13文字以上の推定困難な文字列 b. 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更させる（最長でも2ヶ月以内） c. 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用にPIN等が設定されている場合には、この限りではない。 いずれのパスワードを設定した場合でも、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏えい対策が講じられていることを確認すること。 (5) 類推されやすいパスワードを使用させないこと。また、類似のパスワードを繰り返し使用させないこと。なお、類推されやすいパスワードには、利用者の氏名や生年月日、辞書に記載されている単語等が含まれるものがある。					レ	15②	レ	14⑥	レ
		15. 無線LANを利用する場合、次に掲げる対策を実施すること。 (1) 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。 (2) 不正アクセス対策を実施すること。少なくともMACアドレスによるアクセス制限を実施すること。 (3) 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。 (4) 電波を発する機器（携帯ゲーム機等）による電波干渉に留意すること。			レ	4.2	レ	15⑦	レ	13⑬	
		16. 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) 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。 (3) 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。 (4) 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。			レ	4.2	レ	9④	レ	8⑥	
	D.推奨されるガイドライン	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	レ	4.6	レ	4.2	レ		レ	14.2	レ
		2. 個人情報を入力・参照できる端末から離席する場合、クローズ処理等（クリアスクリーン、ログオフ、パスワード付きスクリーンセーバーの起動等）を実施させること。					レ		レ		レ
		3. 外部のネットワークとの接続点やDBサーバ等の安全管理上の重要部分には、ファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。					レ		レ		レ
		4. 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。 (1) パスワード入力が不成功に終わった場合、再入力に対して一定の不応時間を設定すること。 (2) パスワード再入力の失敗が一定回数を超えた場合、再入力を一定期間受け付けない仕組みとすること。					レ		レ		レ
		5. 利用者認証には、ID・パスワード＋バイオメトリクス又はICカード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように、2つの独立した要素を用いて行う方式（二要素認証）等、より認証強度が高い方式を採用すること。ただし、医療情報システムを利用する端末に二要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか2つ以上）の認証がなされていれば、二要素認証に相当すると考えてよい。					レ	13②	レ	14②	レ
		6. 許可された者以外の無線LANの利用を防止するため、例えば802.1xや電子証明書を組み合わせるなどして、無線LANのセキュリティを強化すること。	レ	4.6			レ	13.4	レ		レ
		7. IoT機器を含む医療情報システムの接続状況や異常発生を把握するため、IoT機器・医療情報システムそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。			レ	4,2	レ	13.4	レ		レ
6.6 人的安全対策	B.考え方	（略）			レ	3.2					
	C.最低限のガイドライン	1. 従業者に対する人的安全管理措置 (1) 法令上の守秘義務のある者以外の者を従業者等として採用するに当たって、雇用契約に守秘・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。	レ	4.4	レ	3.2	レ	7①			
		1. 従業者に対する人的安全管理措置 (2) 従業者に対し個人情報の安全管理に関する教育訓練を定期的に実施すること。	レ	4.4	レ	3.2	レ	7②			
		1. 従業者に対する人的安全管理措置 (3) 従業者の退職後の個人情報保護規程を定めること。	レ	4.4	レ	3.2	レ	7①			
		2. 事務取扱委託業者の監督及び守秘義務契約 (1) 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、個人情報保護のため、次に掲げる対策を実施すること。 a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。 b 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認すること。 c 清掃等の直接医療情報システムにアクセスしない作業の場合でも、作業結果を定期的に確認すること。 d 受託する事業者が再委託を行うか否かを明確にすること。受託する事業者が再委託を行う場合は、受託する事業者と同等の個人情報保護に関する対策及び契約がなされることを条件とすること。			レ	3.2	レ	1② 7③④			
		2. 事務取扱委託業者の監督及び守秘義務契約 (2) ソフトウェアの異常等でデータを救済する必要があるとき等、やむを得ない事情で受託する事業者の保守要員が医療情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。			レ	3.2	レ	7③④			
	D.推奨されるガイドライン	1. サーバ室等の安全管理上重要な場所では、モニタリング等により従業者の行動を管理すること。					レ	8③	レ	12	レ
6.7 情報の破棄	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	3. 6.2章C.1で把握した情報種別ごとに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従業者、具体的な破棄方法を含めること。					レ	8①	レ	7⑨	
		2. 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、読み出し可能な情報がないことを確認すること。					レ	8⑨	レ	7⑩	
		3. 外部保存を受託する事業者等に破棄を委託した場合は、6.6章C.2に従うとともに、確実に情報が破棄されたことを確認すること。					レ	8⑩	レ	7⑪	
		4. 運用管理規程において、不要になった個人情報を含む媒体の破棄に関する規定を定めること。					レ	8⑨			
6.8 情報システムの改造と保守	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 動作確認で個人情報を含むデータを使用するときは、明確に守秘義務を設定するとともに、終了後は確実にデータを消去させること。					レ	15⑨	レ	10①	
		2. メンテナンスを実施するためにサーバに保守事業者の作業員（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。					レ	13⑤	レ	10③	
		3. 保守要員の専用アカウントについて、外部流出等による不正使用の防止の観点から適切に管理することを求めること。					レ	13⑤			レ
		4. 保守要員の離職や担当替え等に応じて速やかに保守要員の専用アカウントを削除できるよう、保守事業者に報告を義務付けるとともに、それに対応できるアカウント管理体制を整備すること。			レ	4.1	レ	13⑤⑦	レ	10③	レ

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		5. 保守事業者がメンテナンスを実施する際には、日単位で作業申請書を事前提出させるとともに、終了時に速やかに作業報告書を提出させること。提出された書類は、医療情報システム安全管理責任者が承認すること。なお、作業申請書の承認は、原則として保守作業の実施前に行う必要があるが、事前に承認を得ずに実施可能なものとして保守事業者と合意したメンテナンスについては、事後承認とすることができる。					レ	15⑧	レ	10.1	レ
		6. 保守事業者と守秘義務契約を締結し、これを遵守させること。			レ	4.1	レ	7③			
		7. 原則として、保守事業者に個人情報を含むデータを医療機関等外等に持ち出させないこと。やむを得ず医療機関等外に持ち出さなければならない場合は、置き忘れ等に対する十分な対策を含む運用管理規程を定めることを求め、医療情報システム安全管理責任者がそれを承認すること。					レ	8⑤	レ	7.1	
		8. リモートメンテナンス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するとともに、当該作業の終了後速やかに医療機関等の責任者が確認すること。					レ	15⑧	レ	10④	
		9. リモートメンテナンス において、やむを得ずファイルを医療機関等へ送付等を行う場合、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。					レ	15⑧	レ	10⑤	
		10. 再委託が行われる場合は、再委託を受ける事業者に対しても、保守事業者の責任で同等の義務を課させること。	レ	4.4	レ	5	レ	1②	レ	3.3	
	D.推奨されるガイドライン	1. 詳細なオペレーション記録を保守操作ログとして記録すること。									レ
		2. 保守作業は医療機関等の関係者の立会いの下で行わせること。									レ
		3. 保守要員と保守事業者との守秘義務契約を求めること。									レ
		4. 保守要員の持ち込む機器や記憶媒体に対して、不正ソフトウェアがないことを確認すること。									レ
		5. 保守事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合には、詳細な作業記録を残すよう求めること。また、必要に応じて、医療機関等の監査に応じるよう求めること。									レ
		6. 保守作業に関わるログの確認の際に、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者の診療録等に何回アクセスされたか確認できる仕組みを備えること。									レ
6.9 情報及び情報機器の持ち出し並びに外部利用について	B.考え方	（略）			レ	2.2、3、4					
	C.最低限のガイドライン	1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しや、BYODの実施に関する方針を運用管理規程で定めること。	レ	4.4	レ	3.2	レ	9⑥	レ	7.1 8.4	
		2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。					レ	8①			
		3. 情報を格納した可搬媒体又は情報機器の盗難、紛失時の対応を運用管理規程に定めること。					レ	8⑦			
		4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底するとともに、教育を実施すること。					レ	7②			
		5. 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すること。					レ	9①②	レ	7⑦	
		6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けるとともに、定期的なパスワードの変更等の対策を実施すること。	レ	4.6	レ	3.2	レ	13⑥	レ	8⑤	
		7. 盗難、置き忘れ等に対応する措置として、情報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。					レ	8⑤	レ	7③	
		8. 持ち出した情報機器について、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、コンピュータウイルス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、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施すること。なお、ネットワークに接続する場合は6.11章の規定を遵守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは6.5章C.15.の基準を満たさないことがあるため、利用できない。ただし、非常時等でやむを得ず公衆無線LANしか利用できない環境である場合に限り、利用を認める。利用する場合は6.11章で述べている基準を満たした通信手段を選択すること					レ	8⑤	レ	7④	
		9. 持ち出した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。					レ	8⑤	レ	7⑥	
		10. 個人保有の情報機器（ノートパソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、医療情報システム安全管理責任者は1～5の対策を行うとともに、医療情報システム安全管理責任者の責任において上記の6、7、8、9と同様の要件を遵守させること。			レ	3.2	レ	9⑥	レ	8.4	
	D.推奨されるガイドライン	1. 外部での情報機器の覗き見による情報の漏えいを避けるため、ディスプレイに覗き見防止フィルタ等を張ること。							レ	12⑥	レ
		2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。							レ		レ
		3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	レ	4.4	レ	3	レ	9⑥	レ	8⑨	レ
		4. ノートパソコン、スマートフォン、タブレット等を持ち出して使用する場合、次に掲げる対策を実施すること。 (1) 紛失、盗難の可能性を十分考慮し、可能な限り端末内に医療情報を置かないこと。やむを得ず医療情報が端末内に存在する場合や、当該端末を利用すれば容易に医療情報にアクセスできる場合は、一定回数パスワード入力を誤った場合に端末を初期化する等の対策を行うこと。 (2) BYODを行う場合は、管理者以外による端末のOSの設定の変更を技術的あるいは運用管理上で制御する等、適切な技術的対策や運用による対策を選択・採用し、十分な安全性が確保された上で行うこと。					レ	9⑥	レ	8⑨	レ
6.10 災害、サイバー攻撃等の非常時の対応	B.考え方	（略）			レ	3.4					
	C.最低限のガイドライン	1. 医療サービスを提供し続けるためのBCPの一環として、“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めておくこと。	レ	4.4	レ	3.4	レ	11①			
		2. 非常時における対応に関する教育及び訓練を従業者に対して行うこと。なお、医療情報システムの障害時の対応についても同様に行うこと。	レ	4.4	レ	3.4	レ	11⑥			
		3. 正常復帰後に、代替手段で運用した間のデータ整合性を図るための規約を用意すること。					レ	11①			
		4. 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。 (1)「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 (2) 非常時機能が定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。 (3) 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。 (4) 医療情報システムに不正ソフトウェアが混入した場合に備えて、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。 (5) 重要なファイルは数世代バックアップを複数の方式で取得し、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。					レ	11④⑤	レ	11①	
		5. 不正ソフトウェアの混入などによる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、必要な対応を行うほか、そのための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。 厚生労働省連絡先 https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html ※ 独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、5. 不正ソフトウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Webサイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先　情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	レ	4.4	レ	3.4	レ	11⑧			
6.11 外部と個人情報を含む	B.考え方	（略）			レ	4					

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
医療情報を交換する場合の安全管理	C.最低限のガイドライン	1. 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。 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。 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対策を実施すること。 上記を満たす対策としては、①クローズドなネットワークを選択する、又は②オープンなネットワークを選択する場合、例えばIPsecとIKEを利用する等してセキュアな通信路を確保すること又は、IPsecによるVPN接続等を利用せず医療情報システムへ接続する場合は、後述の11.に示す方法等により実施すること。 チャネル・セキュリティの確保を閉域ネットワークに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閉域性の範囲を電気通信事業者に確認すること。							レ	13⑨	
		2. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、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た必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、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、Kerberos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。					レ	15⑦	レ	13④	
		3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を実施すること。これに関しては、6.5章で包括的に述べているので、それを参照すること。					レ				
		4. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。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。安全性が確認できる機器とは、例えば、ISO 15408で規定されるセキュリティターゲット又はそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。					レ	15⑦	レ	13⑤	
		5. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても 、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。例えば、S/MIMEの利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。							レ	13⑦	レ
		6. 医療機関等の間の情報通信には、医療機関等だけでなく、電気通信事業者やシステムインテグレータ、運用を受託する事業者、遠隔保守を行う機器保守事業者等の多くの組織が関連する。そのため、次に掲げる事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・ 診療録等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・ 送信元の医療機関等がネットワークに接続できない場合の対処 ・ 送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ ネットワークの経路途中が不通の場合又は著しい遅延が発生している場合の対処 ・ 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・ 伝送情報の暗号化に不具合があった場合の対処 ・ 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・ 障害が起こった場合に障害部位を切り分ける責任 ・ 送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関等内においても、次に掲げる事項を契約や運用管理規程等で定めておくこと。 ・ 通信機器、暗号化装置、認証装置等の管理責任（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・ 患者等に対する説明責任 ・ 事故発生時における復旧作業・他施設やシステムベンダ及びサービス事業者との連絡に当たる専任の管理者の設置 ・ 交換した医療情報等に対する管理責任及び事後責任（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）			レ	4	レ	2①	レ	13①	
		7. 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。			レ	4	レ	7⑥	レ	13⑪	
		8. リモートメンテナンスを実施する場合は、必要に応じて、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等、不必要なログインを防止するための対策を実施すること。 また、サイバー 攻撃への対策については、PCやVPN機器等の脆弱性対策をはじめとする6.5章及び6.6章に記載されている内容や、NISCから示されている「政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）」、2021年4月30日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照すること。メンテナンス自体は6.8章を参照すること。			レ	4	レ	12⑤	レ	10.1 18.1	
		9.電気通信事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質を確認すること。また、上記1及び4を満たしていることを電気通信事業者やオンラインサービス提供事業者に確認すること。			レ	4	レ	15⑩	レ	10.1	
		10.患者等に情報を閲覧させる場合、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個人認証等の対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、ITに係る以外の法令等の遵守の体制等も含めた幅広い対策を立て、それぞれの責任を明確にすること。					レ	8⑧	レ	7⑭	
		11.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。					レ	15⑦	レ	13⑥	
		12. クローズドなネットワークで接続する場合でも、内部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。					レ	15⑦	レ	13③	
		13. 電子署名に用いる秘密鍵の管理は、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うこと。					レ	14②	レ	15.1	
	D.推奨されるガイドライン	1. やむを得ず従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。 2. 共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-2レベル１相当以上の対応を図ること。					レ	8⑧	レ	7.2.1	レ
6.12 法令で定められた記名・押印を電子署名で行うことについて	B.考え方	（略）			レ	4					
	C.最低限のガイドライン	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必要がある。			レ	4	レ	14①			
		1. 以下の電子証明書を用いて電子署名を施すこと (1) A項の要件を満たす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署名等を用いること。 (a) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI認証局の発行する電子証明書を用いて電子署名を施すこと。 保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。 ただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。 (b) 認定認証事業者（電子署名法第2条第3項に定める特定認証業務を行う者として主務大臣の認定を受けた者をいう。以下同じ。）又は認証事業者（電子署名法第2条第2項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下6.12.において同じ）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモー					レ	14①			

第5.2版記載内容			第6.0版									
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A	
		・ 事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、オンラインの場合、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）第3条第1項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ（いずれも本項と同等の電子署名（資格確認を除く）を施すこと）により確認を行うこと。郵送の場合は、身分証明書のコピー（署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること））、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用すること 。 ※　身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか1種類により、又はその他の身分証明書であれば2種類以上により行うこと。 ・ 事業者による利用者の医師等の国家資格保有の確認は、①利用者が保健医療福祉分野PKI認証局の発行する署名用証明書を用いた電子署名を事業者へ提供することによりオンラインで行う方法、②利用者が官公庁の発行した国家資格を証明する書類（以下「国家資格免許証等」という。）の原本又はコピー等（紙媒体の場合は、国家資格免許証等のコピーに署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること）があること 。電子媒体の場合は、本項と同等の電子署名（資格確認を除く）をスキャンしたデータに施すこと。）を事業者へ持参、郵送又は送信する方法、③利用者が電子署名による確認方法以外の電子的に国家資格等情報と連携して提示できる仕組みを用いて事業者へ提示する方法、④利用者の所属又は運営する医療機関等が利用者の国家資格保有の事実の立証を事業者へ行う方法、のいずれかによって利用者の登録時において確認すること（電子署名を行う都度、事業者による医師等の国家資格保有の確認を求めるものではない）。なお、①～③の場合、事業者は、資格確認に用いた国家資格免許証等のコピーや証明書等について、保存年限を定めて保存しておくこと。④の場合、次に掲げる事項が適切					レ	14①				
		－　医療機関等の管理者が、自組織の実在性を事業者に対して立証すること。 －　医療機関等の管理者が国家資格保有の確認を行った者の「氏名、生年月日、性別、住所」（以下「基本４情報」という。）を事業者へ提出すること（これによって、利用者が実在性、本人性及び利用者個人の申請意思を立証した際に、国家資格保有の立証もなされたものとみなすこととする）。 －　医療機関等による医師等の国家資格保有の立証に当たって、医療機関等が責任の主体としての説明責任を果たすため、資格確認を行った実施記録の作成を行うとともに、資格確認を実施した国家資格免許証等のコピーや利用者の基本４情報を提出した書類のコピー等について保存年限を定めて保存し、さらに医療機関等の内部の独立した監査部門による定期的な監査を行うこと。 ・ 事業者が、上記の事項について、適切な外部からの評価を受けていること。 ※　①～④のいずれかによって資格確認を行った後、利用可能となった当該電子署名を利用者が他の事業者に提供した場合、提供を受けた事業者が別途資格の確認を行う必要はない。なお、この場合であっても以下の事項を行うこと。 ・　適切な外部からの評価を受けること。 ・　資格確認に用いた証明書等について、保存年限を定めて保存しておくこと。 (c)「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子 署名に紐づく医師等の国家資格が検証時に電子的に確認できること、当該電子署名を施					レ	14①				
		2. 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、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16年11月）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のものを使用すること。 (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。					レ	14①				
		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」（令和3年4月1日、総務省告示第146号）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」（総務省、平成16年11月）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。 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法定保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。					レ	14①				
7.1 真正性の確保について	B.考え方	（略）			レ	1.1						
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 入力者及び確定者の識別・認証 (1) 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　入力者及び確定者を正しく識別し、認証を行うこと。 b　システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。 c　業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。 (2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合 a　装置の操作者を運用管理規程で明確にするとともに操作者以外のものによる機器の操作を運用上防止すること。 b　当該装置による記録をいつ・誰が行ったか、システム機能と運用の組み合わせにより明確にすること。			レ	1.1	レ	13.⑧ 15⑬				
		2. 記録の確定手順の確立と、識別情報の記録 (1) 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。 (2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合 a　運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。 b　確定された記録が、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。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧		
		3. 更新履歴の保存 (1) 一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。 (2) 同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できるようにすること。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧		
		4. 代行入力の承認機能 (1) 代行入力を実施する場合、具体的にどの業務等に代行入力を認めるか、誰が誰を代行してよいかを運用管理規程で定めること。 (2) 代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。 (3) 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧		

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		5. 機器・ソフトウェアの品質管理 (1) システムがどのような機器、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、システムの仕様を明確に定義すること。 (2) 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。 (3) 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程で定めるとともに、従業者等への教育を実施すること。 (4) 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。			レ	1.1	レ	15⑬	レ	9.2	
	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	6. 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 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が必要である。					レ	15⑦	レ	13⑫	
		7. 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 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。					レ	15⑦ 15⑬	レ	13⑧	
		8. リモートログイン機能を制限すること 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。					レ	8⑧ 15⑬	レ	7⑫	
7.2 見読性の確保について	B.考え方	（略）			レ	1.1					
	C.最低限のガイドライン	1. 情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの全ての情報の所在が日常的に管理されていること。					レ	8④ 15⑬	レ	4①	
		2. 見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である機器、ソフトウェア、関連情報等は常に整備された状態にすること。					レ	15⑬	レ	5④	
		3. 見読目的に応じた応答時間 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にすること。					レ	15⑬	レ	9④	
		4. システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするため、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。			レ	1.1	レ	15⑬	レ	11.2	
	D.推奨されるガイドライン 【医療機関等に保存する場合】	1. バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		2. 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力できるようにすること。									レ
		3. 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップするとともに、そのバックアップデータ等と汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		4. 緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持すること。									レ
		5. 緊急に必要になるとまではいえない診療録等の見読性の確保 緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する事業者の障害等に対応できるような対策を実施しておくこと。									レ
7.3 保存性の確保について	B.考え方	（略）			レ	3、4					
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 不正ソフトウェアによる情報の破壊、混同等の防止 (1) 不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。	レ	4.4	レ	3、4	レ	15⑥ 15⑬	レ	8.1	
		2. 不適切な保管・取扱いによる情報の滅失、破壊の防止 (1) 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。 (2) 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、バックアップ頻度、バックアップ方法等を明確にすること。これらを運用管理規程に定めて、その運用を関係者全員に周知徹底すること。 (3) 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を実施すること。 (4) 電子的に保存された診療録等の情報に対するアクセス履歴を残すとともに、その履歴を適切に管理すること。 (5) 各保存場所における情報が毀損したときに、バックアップされたデータ等を用いて毀損前の状態に戻せるようにすること。もし、毀損前と同じ状態に戻せない場合には、毀損された範囲が容易に分かるようにしておくこと。			レ	3、4	レ	15②③ 15⑬	レ	12.2 18.1	
		3. 記録媒体、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の防止 (1) 記録媒体が劣化する前に、当該記録媒体に保存されている情報を新たな記録媒体又は記録機器に複写すること。記録媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にするとともに、使用開始日、使用終了予定日を管理して、月に一回程度の頻度でチェックを行うこと。使用終了予定日が近づいた記録媒体又は記録機器は、そのデータを新しい記録媒体又は記録機器に複写すること。これら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。					レ	15⑬	レ	12.2	
		4. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 (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こと。 (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。					レ	15⑬	レ	5①	
	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場 合】	5. 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維持しなくてはならない。			レ	3、4	レ	15⑬	レ	5③	
		6. ネットワークや外部保存を受託する事業者に設備の劣化対策の実施を求めること ネットワークや外部保存を受託する事業者の設備の条件を考慮し、回線や設備が劣化した際にそれらを更新する等の対策を実施するよう求めること。			レ	3、4	レ	15⑬	レ	12.2	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
	D. 推奨されるガイドライン【医療機関等に保存する場合】	1. 不適切な保管・取扱いによる情報の滅失・破壊の防止 (1) 記録媒体、記録機器及びサーバは、許可された者しか入ることができない部屋に保管するとともに、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。 (2) サーバ室には、許可された者以外が入室できないよう、鍵等の物理的な対策を施すこと。 (3) 診療録等のデータのバックアップを定期的に取得するとともに、その内容に対する改ざん等が行われていないことを検査する機能を備えること。					レ	8③	レ	12②	レ
		2. 記録媒体、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の防止 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1又はRAID-6相当以上のディスク障害に対する対策を行うこと。									レ
8 診療録及び診療諸記録を外部に保存する際の基準	―						レ	7			
8.1 電子保存の３基準の遵守							レ	1.1.2			
8.2 運用管理規程	B.考え方	（略）			レ	3.2	レ	16			
8.3. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン	1. 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (1) 病院や診療所、医療法人等が適切に管理する場所に診療録等を保存すること。 (2) 委託した医療機関等及び患者等の許可なく、保存を受託した診療録等を分析等の目的で取り扱わせないこと。 (3) 保存を受託した診療録等の分析等は、不当な利益を目的としない場合に限って許可すること。 (4) 匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。 (5) 保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存を受託する事業者に適切なアクセス権を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮するよう求めること。 (6) 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間の同意に基づいて実施すること。			レ	5	レ	7⑦			
		2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合 (1) 保存した情報の取扱いに関して監督できるようにするため、外部保存を受託する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。 (2) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線に関しては6.11章を遵守させること。 (3) 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で確認をすること。 (4) 外部保存を受託する事業者の選定に当たっては、事業者のセキュリティ対策状況を示す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。 (5) 外部保存を受託する事業者に、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。なお保守に関しては、6.8章を遵守すること。 (6) 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するとともに、外部保存を受託する事業者に遵守させること。 (7) 保存した情報を、外部保存を受託する事業者が独自に提供しないように、契約書等で情報提供について定めること。外部保存を受託する事業者が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、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。 (8) 保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。			レ	5	レ	7⑤			
		(9) 外部保存を受託する事業者を選定する際は、(1)から(8)のほか、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認証を取得していること 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機器が設置されている場所(地域、国) i 受託事業者に対する国外法の適用可能性			レ	5	レ	7⑥			
	D. 推奨されるガイドライン	1. ISMS認証を取得している事業者の選定に際しては、選定対象となる事業者に管理しているリスクに応じて、適合性を示す資料の提供を求めること。					レ				レ
		2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保するよう求めること。									レ
		3. 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を備えるよう求めること。									レ
8.4. 個人情報の保護	B.考え方	（略）			レ	4					
	C.最低限のガイドライン	1. 診療録等の外部保存を受託する事業者内における個人情報保護 (1) 委託先を適切に監督すること 診療録等の外部保存を受託する事業者内の個人情報保護については、本ガイドライン6章を参照し、適切な管理を行わせる必要がある。			レ	5	レ	7⑧			
		2. 外部保存実施に関する患者への説明 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、理解を得る必要がある。 (1) 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。 (2) 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。 (3) 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。			レ	1.1、1.2	レ	7⑨			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
9.1. 共通の要件	C.最低限のガイドライン	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、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。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンを行うこと。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版 （平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるため、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像をスキャンした情報はDICOM等の適切な形式で保存すること。					レ	16①	レ	16①	レ
		2. 改ざんを防止するため、次に掲げる対策を実施すること。 (1) スキャナによる読み取りについて運用管理規程に定めること。 (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。 (3) スキャナによる読み取りの際の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こと。なお、電子署名については6.12章を参照すること。			レ	4.1	レ	16①②③			
		3. 情報作成管理者は、運用管理規程に基づき、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。					レ	16④			
9.2. 診療等の都度スキャナ等で電子化して保存する場合	C.最低限のガイドライン	1. 9.1章の対策に加えて、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。 (1) 運用管理規程において、改ざんの動機が生じないと考えられる期間（長くとも1～2日程度以内）を定めるとともに、その期間内に遅滞なくスキャンを行わなければならない。時間外診療等で機器の使用ができない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行う必要がある。			レ	4.1	レ	16⑤			
9.3. 過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合	C.最低限のガイドライン	1. 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すること。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。			レ	4.1	レ	16⑥			
		2. 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。 (1) 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）） (2) 作業責任者 (3) 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 (4) 相互監視を含む実施体制 (5) 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） (6) 事後の監査人と監査項目 (7) 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			レ	4.1	レ	16⑥			
		3. 医療機関等の保有するスキャナ等で電子化を行う場合、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。					レ	16⑥			
		4. 外部事業者に委託する場合は、9.1章の対策と同等以上の安全性を満たすことができる適切な事業者を選定すること。適切な事業者とみなすためには、少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認する必要がある。また、実施に際しては、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の監査を受けることを含め、安全管理に関する条項を契約書等に具体的に明記すること。			レ	4.1	レ	16⑥			
9.4. 紙の調剤済み処方箋をスキャナ等で電子化し保存する場合について	C.最低限のガイドライン	1. 紙の調剤済み処方箋の電子化のタイミングに応じて、9.2章又は9.3章の対策を実施すること。					レ	16⑦			
		2.「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。					レ	16⑦	レ	16.1	
9.5（補足） 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合	C.最低限のガイドライン	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンすること。これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからである。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできる。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版 （平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像情報をスキャンした情報はDICOM等の適切な形式で保存すること。					レ	16⑧	レ	16②	
		2. 情報作成管理者は、運用管理規程を定めて、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。					レ	16⑧			
		3. 緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。					レ	16⑧			
		4. 電子化後の元の紙媒体やフィルムの安全管理を行うこと。					レ	16⑧			
10. 運用管理について	C.最低限のガイドライン	以下の項目を運用管理規程に含めること。本ガイドラインの 4 章から 9 章において「D. 推奨されるガイドライン」に記されている項目は省略しても差し支えない。 1. 一般管理事項			レ	4.1	レ	4.2、8.2.5など			
		2. 電子保存のための運用管理事項			レ	4.1	レ	15③～⑤			
		3. ネットワークによる外部保存に当たっての「医療機関等としての管理事項」 可搬媒体による外部保存、紙媒体による外部保存に当たっては、本項を参照して管理事項を作成すること。			レ	4.1	レ	15④			
		4. スキャナ等により電子化して保存する場合			レ	4.1	レ	16①、③～⑥			
		5. 運用管理規程の作成に当たって			レ	4.1	レ	4.2			