厚労省ガイドライン						クラウドサービス医療ガイドライン		
項目	節				記載内容	項番	サブ項番	ガイドラインとして必要な要求事項
組織的安全管理対策	6.3	C			1. 情報システム運用責任者の設置及び担当者(システム管理者を含む。)の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	3.2.1	(ア)	① サービスの提供についての管理責任を有する責任者を設置する。 ② 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者(システム管理者)を設置する。 ③ サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④ ①から③に掲げた責任者の任命・解任等のルールを策定する。
組織的安全管理対策	6.3	C			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、入退を制限する等の入退管理を定めること。	3.2.2	(ア)2	① サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ② サービスに供する機器や媒体の設置場所への入退状況の管理(入退記録のレビュー含む)は定期的に行う。 ③ サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。 ④ サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤ サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥ サービスに供する機器や媒体の保存場所(ラック、保管庫含む)の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦ ①～⑥につき、運用管理規程等に規定する。
組織的安全管理対策	6.3	C			3. 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。	3.2.1	(エ)1	① クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。 ② サービスの提供に係るアクセス記録(外部からのアクセス、利用者によるアクセス等を含む)の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。
組織的安全管理対策	6.3	C			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。	3.2.1	(イ)2	① サービス提供に係る契約において、次項(ウ)1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。
						3.2.1	(エ)2	① 医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。
組織的安全管理対策	6.3	C			5. 運用管理規程等において次の内容を定めること。 (a) 理念(基本方針と管理目的の表明) (b) 医療機関等の体制 (c) 契約書・マニュアル等の文書の管理 (d) リスクに対する予防、発生時の対応の方法 (e) 機器を用いる場合は機器の管理 (f) 個人情報の記録媒体の管理(保管・授受等)の方法 (g) 患者等への説明と同意を得る方法 (h) 監査 (i) 苦情・質問の受付窓口	3.2.1	(ウ)1	① 経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ② ①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③ ①の指針等には、個人情報保護法の対象外の情報(死者に関する情報等)であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④ 情報セキュリティに係るポリシー等を含む関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤ 情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。 ⑥ 情報セキュリティに関する組織的取組における基本方針セキュリティポリシーについては、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)2	① サービスの提供に係る体制を、緊急時の対応も含めて明確にする。 ② サービスの提供に係る体制等に関する情報(再委託による体制に関する情報を含む)の開示等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)3	① 情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。 ② サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。 ③ サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)4	① サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。 ② サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

						3.2.1	(ウ)5	①　機器等の管理方法について、文書化を行う。 ②　機器等について、台帳管理等により所在確認等を行う旨を定める。 ③　機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)6	①　個人情報を記録した媒体の管理等に関する運用規程を策定する。 ②　個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)7	①　医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)8	①　サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ②　第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③　監査実施について記録し、当該記録の保存･管理方法を明確にする。 ④　自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等に開示する監査記録等の範囲･条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
						3.2.1	(ウ)9	① 医療機関等の管理者からの問合せ窓口を設ける。また受付の時間帯等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化する。
物理的安全管理策	6.4	C			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。	3.2.2	(ア)1	①　サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。 ②　サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③　サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。
物理的安全管理策	6.4	C			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等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。 ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	3.2.2	(ア)2	①　サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ②　サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。 ③　サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。 ④　サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤　サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥　サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦　①～⑥につき、運用管理規程等に規定する。
物理的安全管理策	6.4	C			3.　個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・入退者の記録を定期的にチェックし、妥当性を確認する。	3.2.2	(ア)2	3.2.2(2)(ア)2に統合
物理的安全管理策	6.4	C			4.　個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること。	3.2.2	(ウ)1	①　個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。 ②　個人情報が存在するPC 等の重要な機器には、盗難防止用チェーンを取り付ける。 ③　受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。
物理的安全管理策	6.4	C			5.　窃視防止の対策を実施すること。	3.2.2	(イ)1	①　個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。 ②　運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。

物理的安全管理策	6.4	D			1. 防犯カメラ、自動侵入監視装置等を設置すること。	3.2.2	(ア)4	① サービスに供する機器等が保存されている建物、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する。 ② 防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。 ③ サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。
物理的安全管理策	6.4				明文規定なし	3.2.2	(ア)3	① サービスに供する機器や媒体を物理的に保存するための施設は、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。 ② ①の施設を設置する建築物は、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと	3.2.3	(ア)1	① 情報システムの利用者を特定し識別できるように、アカウントの発行を行う(複数の利用者によるIDの共同利用は行わない。ただし当該情報システムが他の情報システムを利用するためのID(non interactive ID)は除く)。 ② 利用者のなりすまし等を防止するための認証を行う。 ③ 利用者には、医療機関等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。 ④ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行う。
技術的安全管理策	6.5	C			2. 本人の識別・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には、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行うこと。	3.2.3	(ア)2	① 本人の識別・認証に、ユーザIDとパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないにようにする。 ・初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。 ・パスワードの設定に際しては、複数の文字種(英数字・大文字・小文字・記号等)を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。 ② パスワード認証に係る以下のルールを実現する措置を講じる。 ・パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③ パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。 ④ 認証に際してID及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。
技術的安全管理策	6.5	C			3.本人の識別・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には、ICカードの破損等、本人の識別情報が利用できない時を想定し、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。	3.2.3	(ア)4	① 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2要素認証以上の認証強度のある方法による。 ② 利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 利用者の認証において、固定式のID・パスワードによる認証方式を採用している場合には、固定式のID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第5版の公表(平成29年5月)から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。 ④ 利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定める。 ⑤ 代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。 ⑥ 代替的手段・手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。 ⑦ その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			4. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。	3.2.3	(オ)1	① サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。 ② サービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視を行う。 ③ 医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができるようにする。 ⑤ 医療機関等における利用者端末への④の措置の具体的な適用について、サービス仕様適合開示書に基づき、医療機関等と合意する。

技術的安全管理策	6.5	C			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。	3.2.6	(ウ)1	① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。 ② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。
技術的安全管理策	6.5	C			6. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、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適宜行うよう、運用管理規程で定めていること。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担保する必要がある。	3.2.3	(イ)2	① サービスには、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含める。 ② 医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。資料の提供に係る条件等については、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。 情報システムにアクセス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で操作の記録(操作者及び操作内容等)を必ず行うこと。	3.2.3	(エ)1	① 情報システムへのアクセスを記録し、一定期間保存する。 ② アクセス記録には、アクセスしたID、アクセス時刻、アクセス時間、アクセス対象(情報主体単位)等を含める。 ③ アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。 ⑤ ④で定める法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。 ⑥ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。 ⑦ ⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			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講じること。	3.2.3	(エ)2	① アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。 ② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。 ③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。
技術的安全管理策	6.5	C			9. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と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。	3.2.3	(エ)3	① アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。
技術的安全管理策	6.5	C			10. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時には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メディアを利用する際には、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。常時ウイルス等の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。	3.2.3	(カ)1	① 情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。 ⑤ 情報システムの脆弱性に関する情報は、JPCERTコーディネーションセンター(JPCERT/CC)、内閣サイバーセキュリティセンター(NISC)、独立行政法人情報処理推進機構(IPA)等の情報源から、定期的及び必要なタイミングで取得し、確認する。

技術的安全管理策	6.5	C			11. パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。(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) 利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理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い、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)し、本人以外が知りえない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(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。) また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し(最長でも2ヶ月以内※D.5 に規定する2 要素認証を採用している場合を除く。))、極端に短い文字列を使用しないこと。英数字、記号を混在させた8文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと。かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。	3.2.3	(ア)3	① 利用者のパスワード情報は、ハッシュ値での保存を行う等、暗号化手法により、管理する。 ② サービスに供する製品等の導入に際しては、初期パスワードを変更するだけでなく、必要なアカウントの棚卸しを行い、不要なものについては削除を行う。 ③ 利用者がID、パスワードを失念した場合には、予め策定した手順(本人確認を含む)に則り、本人への通知又は再発行を行う。 ④ パスワード等の情報の漏洩が生じた場合又は不正な第三者からの攻撃により漏洩した場合には、直ちに当該IDを無効化し、あらかじめ策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。 ⑤ パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し変更できるような対応を講じる。 ⑥ 利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。 ⑦ 利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するのに必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。 ⑧ 自社において定めたパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			12. 無線LANを利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線LANの利用を特定されないようにすること。例えば、ステルスモード、ANY接続拒否等の対策をとること。 (2) 不正アクセスの対策を施すこと。少なくともSSIDやMACアドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えばWPA2/AES等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線LANの適用に関しては、総務省発行の「一般利用者が安心して無線LANを利用するために」や「企業等が安心して無線LAN を導入・運用するために」を参考にすること。	3.2.3	(コ)1.	① 医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	C			13. IoT 機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT 機器により患者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、適用すること。 (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、対策を講じること。	3.2.3	(コ)2	① IoT機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。 ③ IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。

技術的安全管理策	6.5	D			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。	3.2.3	(イ)1	① 医療情報とそれ以外の情報を区分できる措置を講じる。 ② 医療情報については、情報区分に従ってアクセス制御を行えるようにする。 ③ 仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。 ④ 医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
技術的安全管理策	6.5	D			2. 離席の場合のクローズ処理等を施すこと(クリアスクリーン:ログオフあるいはパスワード付きスクリーンセーバー等)。	3.2.3	(オ)1	3.2.3(2)(オ)1に統合
技術的安全管理策	6.5	D			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。	3.2.3	(カ)2	① 外部のネットワークと医療情報を格納する機器との接続に際しては、セキュリティゲートウェイ(ネットワーク境界に設置したファイアウォール、ルータ等)を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。 ② 医療機関等との接続ネットワーク境界には、侵入検知システム(IDS)、侵入防止システム(IPS)等を導入してネットワーク上の不正なイベントを検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③ 侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。 ④ ホスティングの利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。
技術的安全管理策	6.5	D			4. パスワードを利用者識別に使用する場合以下の基準を遵守すること。 (1) パスワード入力が不成功に終わった場合の再入力に対して一定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は再入力を一定期間受け付けない機構とすること。	3.2.3	(ア)2	3.2.3(2)(ア)2に統合
						3.2.3	(オ)1	3.2.3(2)(オ)1に統合
						3.2.3	(オ)1	3.2.3(2)(オ)1に統合
技術的安全管理策	6.5	D			5. 認証に用いられる手段としては、ID＋バイオメトリックスあるいはICカード等のセキュリティ・デバイス＋パスワードまたはバイオメトリックスのように利用者しか持ち得ない2つの独立した要素を用いて行う方式(2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、情報システムを利用する端末に2 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2 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、2 要素認証と同等と考えてよい。	3.2.3	(ア)4	3.2.3(2)(ア)4に統合
技術的安全管理策	6.5	D			6. 無線LANのアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば802.1xや電子証明書を組み合わせたセキュリティ強化をすること。	3.2.3	(コ)2	3.2.3(2)(コ)2に統合
技術的安全管理策	6.5	D			7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムが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。	3.2.3	(コ)2	3.2.3(2)(コ)2に統合

人的安全管理対策	6.6 (1) 従業者に対する人的安全管理措置	C			1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。	3.2.4	(ア)1	①　サービスの提供に従事する要員(被用者、派遣従業者等)については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。
人的安全管理対策	6.6 (1) 従業者に対する人的安全管理措置	C			2. 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。	3.2.4	(ア)2	①　サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。 ②　この教育・訓練は就業開始時及び就業後定期的に行う。
						3.2.4	(ア)5	①　サービスの提供に従事する要員に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
人的安全管理対策	6.6 (1) 従業者に対する人的安全管理措置	C			3. 従業者の退職後の個人情報保護規程を定めること。	3.2.4	(ア)3	①　サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。 ②　サービスの提供に従事する要員が業務上管理していた個人情報については、離職時(内部の異動含む)に返却を求め、システム管理者が返却されたことを確認する。 ③　サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記2.における教育・訓練に含める。
人的安全管理対策	6.6 (1) 従業者に対する人的安全管理措置	D			1.　サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。	3.2.2	(ア)1	3.2.2(2)(ア)4に統合
人的安全管理対策	6.6 (2) 事務取扱委託業者の監督及び守秘義務契約	C			1.　病院事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること ② 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・作業結果の確認を行うこと。 ③ 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においても、作業後の定期的なチェックを行うこと。 ④ 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託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ていることを条件 とすること。	3.2.4	(ア)4	①　上記1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。
						3.2.4	(イ)1	①　情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。 ②　再委託先には、自社と同等の個人情報保護指針等を遵守させる。 ③　再委託に係る契約に、委託業務に係る守秘義務を含める。 ④　再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。 ⑤　再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。
						3.2.6	(イ)2	①　情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。 ②　取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。
人的安全管理対策	6.6 (2) 事務取扱委託業者の監督及び守秘義務契約	C			2.　プログラムの異常等で、保存データを救済する必要があるとき等、やむを得ないえない事情で外部の保守要員が診療録等の個人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。	3.2.4	(ア)4	3.2.4(2)(ア)4に統合
情報の破棄	6.7	C			1. 「6.1 方針の制定と公表」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の特定、具体的な破棄の方法を含めること。	3.2.5	(ア)2	①　情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。 ②　再委託先には、自社と同等の個人情報保護指針等を遵守させる。 ③　再委託に係る契約に、委託業務に係る守秘義務を含める。 ④　再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。 ⑤　再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。

情報の破棄	6.7	C			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とし、残存し、読み出し可能な情報がないことを確認すること。	3.2.5	(ア)1	① サービスに供する情報を格納する機器、媒体等を破棄する手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。 ② 情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法(電磁記録媒体の消磁･物理的破壊等)を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。 ③ ①で講じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報の破棄	6.7	C			3. 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策(2)事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。	3.2.5	(ア)1	3.2.5(2)(ア)1に統合
情報の破棄	6.7	C			4. 運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成	3.2.5	(ア)2	3.2.5(2)(ア)2に統合
情報システムの改造と保守	6.8	C			1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	3.2.6	(ウ)1	3.2.6(2)(ウ)1に統合
情報システムの改造と保守	6.8	C			2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別･認証についても同様である。	3.2.6	(ア)1	① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。 ② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。
情報システムの改造と保守	6.8	C			3. そのアカウント情報は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。	3.2.6	(ア)2	① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。
情報システムの改造と保守	6.8	C			4. 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。	3.2.6	(オ)1	① 情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報システムの改造と保守	6.8	C			5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	3.2.6	(イ)4	① 情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② ①における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。 ③ 保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。 ④ ③に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ ④で示された手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑥ 保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報システムの改造と保守	6.8	C			6. 保守会社と守秘義務契約を締結し、これを遵守させること。	3.2.1	(イ)1	① サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。

情報システムの改造と保守	6.8	C			7. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	3.2.6	(ウ)2	① 医療情報を格納する機器等を、保守(例えば機器の修理等)の目的で、医療機関等又はクラウドサービス事業者等(再委託事業者含む)の組織外に持ち出す必要がある場合には、その手順を策定する。 ② ①で定める手順及び情報の提供条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報システムの改造と保守	6.8	C			8. リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	3.2.6	(イ)1	① リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。 ② リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。 ③ サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報システムの改造と保守	6.8	C			9. 再委託が行われる場合は再委託する事業者にも保守会社と同等の義務を課すこと。	3.2.6	(オ)2	① 情報システムの保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。 ② ①の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。
情報システムの改造と保守	6.8	D			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。	3.2.6	(イ)2	3.2.6(2)(イ)2に統合
情報システムの改造と保守	6.8	D			2. 保守作業時には病院医療機関等の関係者立会いのもと下で行うこと。	3.2.6	(イ)3	① 情報システムの保守業務を医療機関等の施設内で行う際の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報システムの改造と保守	6.8	D			3. 作業員各人と保守会社との守秘義務契約を求めること。	3.2.4	(ア)1	3.2.4(2)(ア)1に統合
情報システムの改造と保守	6.8	D			4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織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ことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。	3.2.6	(ウ)2	3.2.6(2)(ウ)2に統合
情報システムの改造と保守	6.8	D			5. 保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。	3.2.6	(イ)2	3.2.6(2)(イ)2に統合
情報および情報機器の持ち出し	6.9	C			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に関する方針を運用管理規程で定めること。	3.2.7	(ア)1	① サービスに関する情報(受託情報、情報システムに関連する情報等)を格納する機器・媒体等の持ち出し(委託元からの持ち出しを含む)に関する方針及び規則等を、運用管理規程に定める。 ② ①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。 ③ ①で定める内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
情報および情報機器の持ち出し	6.9	C			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。	3.2.7	(ア)2	① サービスに供する記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体・記録機器の取扱い ・サービスに関する情報(受託情報、情報システムに関連する情報等)を格納する機器・媒体等の持ち出し(委託元からの持ち出し含む)に関する方針及び規則等(「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。) ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失(持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等(第三者による悪意の送信、従業者等における誤送信等を含む。))が起きた場合の対応 ・外部のネットワークに接続する場合の接続条件、安全管理措置等(格納された情報の漏洩や改ざんが生じないようにするための具体的な措置(マルウェア対策、暗号化、ファイアウォール導入等))

情報および情報機器の持ち出し	6.9	C			3. 情報を格納した可搬媒体もしく若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。	3.2.7	(ア)2	3.2.7(2)(ア)2に統合
情報および情報機器の持ち出し	6.9	C			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し、教育を行うこと。	3.2.7	(ア)3	① 「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ② 上記の運用管理規程については、再委託先に対しても遵守等を求める。
情報および情報機器の持ち出し	6.9	C			5. 医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。	3.2.7	(イ)	① サービスに関する情報を格納する機器・媒体等については、台帳管理等を行い、定期的に所在確認を行う。
情報および情報機器の持ち出し	6.9	C			6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。	3.2.7	(ウ)1	① サービスに供する機器等については、起動パスワードの設定を行う。 ② 起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。 ③ サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。
情報および情報機器の持ち出し	6.9	C			7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。	3.2.7	(ウ)2	① サービスに関する情報を格納する機器・媒体等を持ち出す場合の手順には、機器・媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。
情報および情報機器の持ち出し	6.9	C			8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、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施すこと。なお、ネットワークに接続する場合は「6. 11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。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-11 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、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。	3.2.7	(ウ)5	① 業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。
情報および情報機器の持ち出し					対応要求事項削除			–
情報および情報機器の持ち出し	6.9	C			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あるいは停止するか、業務に対して影響がないことを確認して用いること。	3.2.7	(ウ)3	① サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。 ② サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。
情報および情報機器の持ち出し	6.9	C			10. 個人保有の情報機器（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、、管理者は1～5 の対策を行うとともに、管理者の責任において上記の6、7、8、9と同様の要件を順守させること。	3.2.7	(ウ)4	① サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止する。 ② 利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する。 なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏えい等を防止する観点から、例えば、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。
情報および情報機器の持ち出し	6.9	D			1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。	3.2.2	(イ)1	3.2.2(2)(イ)1に統合
情報および情報機器の持ち出し	6.9	D			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。	3.2.7	(ウ)1	3.2.7(2)(ウ)1に統合

情報および情報機器の持ち出し	6.9	D			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。	3.2.7	(イ)	3.2.7(2)(イ)に統合
情報および情報機器の持ち出し	6.9	D			4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者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は端末を初期化する等の対策を行うこと。	3.2.7	(ウ)4	3.2.7(2)(ウ)4に統合
情報および情報機器の持ち出し					6.9全般	3.2.7	(ア)4	① 「2.サービスに供する記録媒体・記録機器に関する対応」、「3.従業員等及び委託先に対する対応」に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。
災害等の非常時の対応	6.10	C			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”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	3.2.8	(イ)1	① サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ② ①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。 ③ ①で策定したBCP及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
災害等の非常時の対応	6.10	C			2. 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規約を用意すること。	3.2.8	(イ)4	① 非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の規定等）を講じる。
災害等の非常時の対応	6.10	C			3. 非常時の情報システムの運用 ・「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。 ・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し、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。 ・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出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、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。	3.2.8	(イ)2	① 非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。 ③ 非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。 ④ 非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。
災害等の非常時の対応	6.10	C			4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。 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。 連絡先厚生労働省医政局研究開発振興課医療技術情報推進室（03-3595-2430）※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、マル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）	3.2.8	(イ)3	① サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。 ② ①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。 ③ ①の場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関と合意する。 ④ ③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する。

外部と個人情報を含む医療情報を交換する場合	6.11	C			1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこととること。 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とること。 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とること。 上記を満たす対策として、例えばIPSec とIKE を利用することによりセキュアな通信路を確保することがあげられる。 チャネル・セキュリティの確保を閉域ネットワークの採用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事業者に確認すること。	3.2.9	(ア)1	①　ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う。 ②　アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。 ③　経路の安全性確保のため、IPSec + IKEへの対応や閉域ネットワークへの対応等及びその条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等がチャネル・セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			2.　データ送信元と送信先での、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。認証手段としては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の容易に解読されない方法を用いるのが望ましい。	3.2.9	(ア)2	①　医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。 ②　①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認証を行う。 ③　①について、事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策を講じる。 ④　厚生労働省ガイドライン第5版6.11 C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			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とること。これに関しては、医療情報の安全管理に関するガイドライン「6.5技術的安全対策」で包括的に述べているので、それを参照すること。	3.2.3		3.2.3②で包括的に対応
外部と個人情報を含む医療情報を交換する場合	6.11	C			4.　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し、施設内のルータを経由して異なる施設間を結ぶVPNの間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408で規定されるセキュリティターゲットもしく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。	3.2.9	(ア)3	①　ルータ等のネットワーク機器は、ISO15408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文書が、本ガイドラインに適合しているものを選定する。 ②　ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関するクラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			5.　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。たとえば、SSL/TLSの利用、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。	3.2.9	(ア)4	①　送信元と相手先の当事者間で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。 ②　サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。 ③　②のほか、メールの暗号化（S/MIME等）やファイルの暗号化への対応を医療機関等が求める場合には、その対応に必要な措置及び条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

外部と個人情報を含む医療情報を交換する場合	6.11	C			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、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。 そのため、次の事項について、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。 ・診療情報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または著しい遅延の場合の対処 ・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また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、医療機関内においても次の事項において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の明確化（。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の明確化。 ・事故発生時における復旧作業・他施設やベンダ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の明確化（。 ・ 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）。	3.2.9	（ウ）1	①　通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ②　交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③　医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			7. 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を行って不必要なログインを防止すること。	3.2.9	（イ）1	①　リモートメンテナンスにより保守を行う場合、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の安全管理措置を講じる。
外部と個人情報を含む医療情報を交換する場合	6.11	C			8. 回線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に関して問題がないか確認すること。また上記1及び4を満たしていることを確認すること。	3.2.9	（ア）6	①　回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			9. 患者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、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた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の納得できる説明を実施し、ITに係る以外の法的根拠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。	3.2.9	（ウ）2	①　サービスにより管理する医療情報を患者等の閲覧に供する場合に、クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ②　医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③　患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部と個人情報を含む医療情報を交換する場合	6.11	C			10. オープンなネットワークを介してHTTPS を利用した接続を行う際、IPsec を用いたVPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLSのプロトコルバージョンをTLS1.2 のみに限定した上で、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。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」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。いわゆるSSL-VPNは偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型のIPsec 若しくはTLS1.2 により接続する場合、セッション間の回込み（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）等による攻撃からの防護について、適切な対策を実施すること。	3.2.9	（ア）5	①　オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。 ②　SSL-VPNは、原則として使用しない。 ③　サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 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）等による攻撃について、適切な対策を実施する。 ④　医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 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）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

外部と個人情報を含む医療情報を交換する場合	6.11	D			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共に運用等の要件を設定すること。	3.2.9	（ア）7	① 医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担等につき、サービス仕様適合開示書に基づき、医療機関等と合意する。
法令で定められた記名・押印を電子署名で行うこと	6.12	C			（1）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認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと 1. 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。従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ことが推奨 される。 ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。 2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件 を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。 3.「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、行政機関以外に当該電子署名を検証しなければならない者が全て公的個人認証サービスを用いた電子署名を検証できることが必要である。	3.2.10	（ア）	① 法令で署名又は記名･押印が義務付けられた文書等において、記名･押印を電子署名に代える場合に、保健医療福祉分野PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。 ② 保健医療福祉分野PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名･押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「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1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名･押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
法令で定められた記名・押印を電子署名で行うこと	6.12	C			（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、「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し、第三者がタイムスタンプを検証することが可能であること。 2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。 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講じる必要がある。	3.2.10	（イ）	① 電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容･検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
法令で定められた記名・押印を電子署名で行うこと	6.12	C			（3）上記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. 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。本来法的な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に、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共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。	3.2.10	（ウ）	① タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
真正性の確保	7.1	C	（1）入力者及び確定者の識別及び認証	a. 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	1. 入力者及び確定者を正しく識別し、認証を行うこと。	3.2.3	（ウ）(a)1	① e-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様

真正性の確保	7.1	C	(1) 入力者及び確定者の識別及び認証	a. 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	2. 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、権限のある利用者以外による作成、追記、変更を防止すること。	3.2.3	(ウ)(a)1	3.2.3(2)(ウ)(a)1に統合
真正性の確保	7.1	C	(1) 入力者及び確定者の識別及び認証	a. 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	3. 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。	3.2.3	(ウ)(a)1	3.2.3(2)(ウ)(a)1に統合
真正性の確保	7.1	C	(1) 入力者及び確定者の識別及び認証	b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置もしくはシステムにより記録が作成される場合	1. 装置の管理責任者や操作者が運用管理規程で明確にされ、管理責任者、操作者以外による機器の操作が運用上防止されていること。	3.2.3	(ウ)(a)2	① e-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・サービスとの連携におけるインタフェースの構築に関する役割分担
真正性の確保	7.1	C	(1) 入力者及び確定者の識別及び認証	b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置もしくはシステムにより記録が作成される場合	2. 当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	3.2.3	(ウ)(a)2	3.2.3(2)(ウ)(a)2に統合
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任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が含まれること。	3.2.3	(ウ)(b)1	① e-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・確定された登録情報(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)に関する仕様 ・入力された内容についての記録確定前における確認の可否等についての仕様 ・記録の確定権限に関する仕様 ・確定した記録の追記・削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	2. 「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	3.2.3	(ウ)(b)1	3.2.3(2)(ウ)(b)1に統合

真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	3.「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。	3.2.3	(ウ)(b)1	3.2.3(2)(ウ)(b)1に統合
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	4. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	3.2.3	(ウ)(b)1	3.2.3(2)(ウ)(b)1に統合
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	5. 一定時間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策定し運用管理規程に明記すること。	3.2.3	(ウ)(b)1	3.2.3(2)(ウ)(b)1に統合
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	a. 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	6. 確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の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で定め、記録の確定の責任の所在を明確にすること。	3.2.3	(ウ)(b)1	3.2.3(2)(ウ)(b)1に統合
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	b. 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	1. 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が定義されていること。その際、作成責任者の氏名等の識別情報（または装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。			–
真正性の確保	7.1	C	(2) 記録の確定手順の確立と、識別情報の記録	b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置もしくはシステムにより記録が作成される場合	2. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。			–
真正性の確保	7.1	C	(3) 更新履歴の保存		1. 一旦確定した診療録等を更新した場合、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せることができること。	3.2.3	(ウ)(c)1	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含める。
真正性の確保	7.1	C	(3) 更新履歴の保存		2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	3.2.3	(ウ)(c)2	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。

真正性の確保	7.1	C	(4) 代行操作の承認機能		1. 代行操作を運用上認めるケースがあれば、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	3.2.3	(ウ)(d)	① 真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 真正性が求められる医療情報を取り扱うサービスには、代行入力の内容(代行者及び被代行者、代行対象となった記録、代行の日時等)を記録する機能を含める。 ③ 真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作(承認)に関する機能を含める。
真正性の確保	7.1	C	(4) 代行操作の承認機能		2. 代行操作が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行操作の都度記録されること。	3.2.3	(ウ)(d)	3.2.3(2)(ウ)(d)に統合
真正性の確保	7.1	C	(4) 代行操作の承認機能		3. 代行操作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)」が行われること。	3.2.3	(ウ)(d)	3.2.3(2)(ウ)(d)に統合
真正性の確保	7.1	C			4.削除			−
真正性の確保	7.1	C	(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が明らかにされており、システムの仕様が明確に定義されていること。	3.2.3	(ケ)1	① 情報システムにおける機器及びソフトウェアの構成図を作成する。 ② 情報システムのネットワーク構成図を作成する。 ③ ①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。 ④ 情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。 ⑤ ①～④で策定した資料等を医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を医療機関等と合意する。
真正性の確保	7.1	C	(5) 機器・ソフトウェアの品質管理		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が規定されていること。	3.2.3	(ケ)1	3.2.3(2)(ケ)1に統合
真正性の確保	7.1	C	(5) 機器・ソフトウェアの品質管理		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に盛り込み、従業者等への教育を実施すること。	3.2.3	(ケ)2	① サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。 ② サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。 ③ サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。 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の内容、手順等を運用管理規程等に含める。
真正性の確保	7.1	C	(5) 機器・ソフトウェアの品質管理		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。	3.2.3	(ケ)2	3.2.3(2)(ケ)2に統合
真正性の確保	7.1	C	【ネットワークを通じて医療機関等の外		(1) 通信の相手先が正当であることを認識するための相互認証をおこなうこと 診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、	3.2.9	(ア)2	3.2.9(2)(ア)2に統合
真正性の確保	7.1	C	【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】		(2) 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こと。なお、可逆的な情報の圧縮・回復ならびにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。	3.2.9	(ア)4	3.2.9(2)(ア)4に統合
真正性の確保	7.1	C	【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】		(3) リモートログイン機能を制限すること 保守目的等のどうしても必要な場合を除き行なえないように、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。 なお、これらの具体的要件については、「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。	3.2.6	(イ)1	3.2.6(2)(イ)1に統合
見読性の確保	7.2	C	(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、患者毎の情報の全ての所在が日常的に管理されていること。	3.2.3	(イ)3	① サービスには、受託する医療情報を患者等ごとに管理できる機能を含める。
見読性の確保	7.2	C	(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は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	3.2.3	(ク)5	① 医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。 ② 受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合(媒体の劣化、読取装置等のサポート切れ等)、速やかに代替的な措置を講じ、見読性確保のための対応を行う。

見読性の確保	7.2	C	(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もしくは書面に表示できること。	3.2.3	(キ)	① 医療機関等がサービスを利用する際の、応答時間(一般的な表示速度、検索結果の表示時間等)について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2		(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に、システムの冗長化や代替え的な見読化手段を用意すること。	3.2.3	(ク)3	① 情報システム、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。 ② 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、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。 ③ ①を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2	C	【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することができること。	3.2.8	(ア)2	① 医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2	C	【医療機関等に保存する場合】	(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することができること。	3.2.8	(ア)3	① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2	C	【医療機関等に保存する場合】	(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し、そのバックアップデータ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することができること。	3.2.8	(ア)4	① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2	C	【ネットワークを通じて外部に保存する場合】	(1)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、外部に保存しても複製または同等の内容を医療機関等の内部に保持すること。	3.2.8	(ア)5	① 緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
見読性の確保	7.2	C	【ネットワークを通じて外部に保存する場合】	(2)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機関の障害等に対応できるような措置を行っておくこと。	3.2.8	(ア)1	① 障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。
保存性の確保	7.3	C	【医療機関等に保存する場合】	(1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。	3.2.3	(カ)1	3.2.3(2)(カ)1に統合
保存性の確保	7.3	C	【医療機関等に保存する場合】	(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は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に関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。	3.2.7	(ア)2	3.2.7(2)(ア)2に統合

保存性の確保	7.3	C	【医療機関等に保存する場合】	(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	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用量(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示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。	3.2.3	(ク)1	① 各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。 ② 医療機関等がサービスを利用する際に、利用可能な資源に係る情報(保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等)について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 情報システムが情報を保存する場所(内部、可搬媒体)、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。 ④ ③において、他の事業者が提供するクラウドサービスを利用する場合においても、同様の情報を収集して、対応する。仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。 ⑤ ③により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。 ⑥ サービスに係る委託先に対しても、③の運用管理規程に定める管理方法への対応等を求める。
保存性の確保	7.3	C	【医療機関等に保存する場合】	(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	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施すこと。	3.2.2	(ア)2	3.2.2(2)(ア)2へ統合
保存性の確保	7.3	C	【医療機関等に保存する場合】	(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	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し、管理すること。	3.2.3	(エ)1	3.2.3(2)(エ)1へ統合
保存性の確保	7.3	C	【医療機関等に保存する場合】	(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	5. 各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	3.2.3	(ク)4	① 情報が毀損した場合、速やかに回復するための措置を講じ、その内容･手順等について、運用管理規程等に含める。 ② ①に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。 ③ ②で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
保存性の確保	7.3	C	【医療機関等に保存する場合】	(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以前に情報を新たな記録媒体または記録機器に複写すること。記録する媒体及び機器毎に劣化が起こらずに正常に保存が行える期間を明確にし、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体または記録機器については、そのデータを新しい記録媒体また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まとめて記載し、関係者に周知徹底すること。	3.2.3	(ク)2	① 3. 2. 1(2)(ウ)4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法･媒体、管理方法等を定め、その内容を運用管理規程等に含める。 ② ①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん･破壊等がないことを確認する。 ③ 記録媒体に格納するバックアップについては、その媒体の特性(テープ／ディスクの別、容量等)を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。 ④ ③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。 ⑤ ①～④の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。 ⑥ バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。
保存性の確保	7.3	C	【医療機関等に保存する場合】	(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、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	3.2.6	(エ)1	① 診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格(以下、「厚生労働省標準規格」という。)が定められているものについては、それを採用する。 ② 厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、サービス仕様適合開示書に基づき、医療機関等と合意する。
保存性の確保	7.3	C	【医療機関等に保存する場合】	(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	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ていること。	3.2.6	(エ)2	① 医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える。 ② ①に示す機能等を備えることが困難な場合の情報システム更新･移行の手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。

保存性の確保	7.3	C	【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】		(1)データ形式及び転送プロトコルのバージョン管理と継続性の確保をおこなうこと 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または変更されることが考えられる。その場合、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。	3.2.6	(エ)3	① データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。 ② ①の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。 ③ ②は、他の情報システムとのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、3．4に示す対策を講じる。
保存性の確保	7.3	C	【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】		(2)ネットワークや外部保存を受託する機関の設備の劣化対策をおこなうこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。	3.2.6	(エ)4	① サービスに供する情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。 ② サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。 ③ サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ④ ③においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
保存性の確保	7.3	D	【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. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、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。	3.2.2	(ア)2	3.2.2(2)(ア)2へ統合
保存性の確保	7.3	D	【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	2. サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。	3.2.2	(ア)1	3.2.2(2)(ア)1へ統合
保存性の確保	7.3	D	【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	3. 診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。	3.2.3	(ク)2	3.2.3(2)(ク)2に統合
保存性の確保	7.3	D	【医療機関等に保存する場合】	(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もしくはRAID-6相当以上のディスク障害に対する対策を取ること。	3.2.3	(ク)3	3.2.3(2)(ク)3に統合
保存性の確保	7.3	D	【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】		(1) ネットワークや外部保存を受託する機関の設備の互換性を確保すること 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。	3.2.6	(エ)5	① 医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。 ② 他のクラウドサービス事業者が提供するクラウドサービスを用いて、サービスを提供する場合には、他のクラウドサービス事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他のクラウドサービス事業者のクラウドサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、「4. サービスに供する機器の劣化対策」②～④に示す対応策を講じる。 ③ 医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他のクラウドサービス事業者のクラウドサービスの変更を行う場合には、①、②を考慮して行う。

保存性の確保	8.1.2	C	③ 医療機関等が民間事業者等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		(ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。	3.2.1	(イ)1	3.2.1(2)(イ)1に統合
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(イ) 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の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。	3.2.9		3.2.9で包括的に対応
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等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。	3.2.1	(イ)3	① サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。 ② ①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な限り具体的に行う(例えば、総務省が定める「ASP・SaaS(医療情報取扱いサービス)の安全・信頼性に係る情報開示指針」(平成29年3月31日)に定める事項に準じた情報の提供を行う等)
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。	3.3.6	(イ)1	① 受託した医療情報を保守・運用を行うために閲覧するのは必要最小限とする。 ② ①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前・事後の承認により実施する。 ③ 受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。 ④ ①～③における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また②、③により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。	3.3.6	(ウ)1	① 受託した医療情報の解析・分析は、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。 ② 受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等において情報提供について規定すること。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、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。	3.3.6	(ウ)2	① 受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。 ② ①の内容を、サービス提供に係る契約に含める。 ③ 医療機関等の指示に基づき、受託した医療情報の第三者提供(閲覧)を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように、3．2．3及び3．2．9に示す対応策を講じる。 ④ ③により、第三者提供(閲覧)を行う場合には、閲覧・取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者(医療情報連携ネットワーク等)の指示に基づき、速やかに変更・削除できる対応を行う。 ⑤ 医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容(提供先(閲覧者)、閲覧情報、閲覧日時等)の報告を行う。 ⑥ ①～⑤により第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	C	③ 医療機関等が民間事業者等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		(キ) 医療機関等において(ア)から(カ)を満たした上で、外部保存を受託する事業者の選定基準を定めること。尐なくとも以下の4 点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 (b) 医療情報等の安全管理に係る実施体制の整備 (c) 実績等に基づく個人データ安全管理に関する信用度 (d) 財務諸表等に基づく経営の健全性	3.3.6	(ア)	① サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。 ・医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況 ・医療情報等の安全管理に係る実施体制の整備状況 ・実績等に基づく個人データ安全管理に関する信用度 ・財務諸表等に基づく経営の健全性

外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	D			(ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」では、技術的な方法としては、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こと。	3.3.6	(イ)2	①　予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。 ②　システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置(データベースの暗号化等)を講じる。
外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準	8.1.2	D			(エ) 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、「(a)暗号化を行う」、「(b)情報を分散管理する」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併せ持つこと。	3.3.6	(イ)2	3.3.6(2)(イ)2に統合
個人情報の保護	8.1.3	C	(1) 診療録等の外部保存委託先の事業者内における個人情報保護		① 適切な委託先の監督を行なうこと 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、適切な管理を行う必要がある。	3.3.7	(ア)	①　個人情報保護対応策を、サービス仕様適合開示書に基づき、医療機関等と合意する。
個人情報の保護	8.1.3	C	(2)外部保存実施に関する患者への説明	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べきである。	3.3.7	(イ)	①　医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。
個人情報の保護	8.1.3	C		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し、理解を得ればよい。			–
個人情報の保護	8.1.3	C		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。			–
個人情報の保護	8.4.2				診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。 これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。 これらの厳正な取り扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になりうるためであり、そのことに十分に留意しなければならない。 ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。 また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。	3.4		①　サービスの一部又は全部の停止やサービス変更の場合(軽微なバージョンアップは含まない)には、サービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ②　①の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲(データ種類、期間等)、データ形式(データ項目、項目の詳細、ファイル形式)、返却方法、条件については、サービス仕様適合開示書に基づき、医療機関等と合意する。また医療機関等のサービス利用開始後に、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。 ③　②におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮(画像データ等)や変換(パスワード等)によるデータが含まれる場合があるので、その旨も合わせて、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　①においてサービスの変更を含むサービスの一部又は全部の停止(軽微なバージョンアップは含まない)が生じる場合の医療機関等への対応の内容(移行支援等で、②の対応は除く)、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等の都合により医療機関等のサービス利用が終了する場合も、②、③に示す対応策を講じる。 ⑥　サービス提供の停止又は医療機関等におけるサービス利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。 ⑦　⑥に関して、医療機関等へのサポート(所管官庁への情報提供含む)等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑧　①～⑦についての手順等を、運用管理規程等に含める。