別紙5

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.1	（ア）	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。	7.3	組織的安全管理策（体制、運用管理規程）	実施すべき安全管理策	（1）医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。 （2）個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。 （3）個人情報保護に関しては、医療機関等の監督の下に行うこと。 （4）情報処理の安全管理に関わる手順書、運用管理規程を整備すること。 （5）運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。
	（イ）1	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。				
		保存性の確保	8.1.2	C		（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。				
	（イ）2	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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）3	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		(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。				
	（ウ）1	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。				
		組織的安全管理対策	6.3	C		(a) 理念（基本方針と管理目的の表明）	7.3	組織的安全管理策（体制、運用管理規程）	実施すべき安全管理策	(1)医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。 (2)個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
	（ウ）2	組織的安全管理対策	6.3	C		(b) 医療機関等の体制				
	（ウ）3	組織的安全管理対策	6.3	C		(c) 契約書・マニュアル等の文書の管理	7.3	組織的安全管理策（体制、運用管理規程）	実施すべき安全管理策	(4)情報処理の安全管理に関わる手順書、運用管理規程を整備すること。 (5)運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理(保管・授受等)、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。
							7.2.1	資産台帳	実施すべき安全管理策	(1)医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。 (2)預託された情報の全てを資産台帳に記録すること。 (3)必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。 (4)資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。 (5)資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
							7.2.1	資産台帳	推奨される安全管理策	(1)資産台帳等を紙文書として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について検出・記録できるような仕組みを実装することが望ましい。 (2)資産台帳等に記録する情報には次のようなものが考えられる。 ●整理番号 ●資産の名称(医療情報の名称) ●資産の医療情報としての種別 ●データ形式及び見読化手段 ●資産の所在地と複製の可否及び複製の所在地 ●資産を保存する情報処理装置、電子媒体の識別番号等 ●資産を扱う医療機関等業務の概要 ●情報処理事業者における管理責任者 ●設定されたアクセス権限とアクセス権限者 ●資産の発生日時、保有する期限、廃棄予定日 ●資産に対する処理の履歴(保存、配送、複製、廃棄等)
	(ウ)4	組織的安全管理対策	6.3	C		(d) リスクに対する予防、発生時の対応の方法	7.10.1	要求事項の識別	実施すべき安全管理策	(1) 医療情報処理に関わる業務プロセス(プロセスを実施するための作業員を含む)、情報処理装置等について識別すること。 (2) 業務プロセス間の相互関係を評価すること。 (3) 事業を継続するための業務プロセスの優先順位を明確にすること。 (4) 医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。 (5) 医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。
							7.6.7	電子媒体の取扱	推奨される安全管理策	(1)物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。
							7.2.2	情報の分類	実施すべき安全管理策	(3)預託される情報に対して分類にもとづいたリスク分析を実施すること。 (4)リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。
	(ウ)5	組織的安全管理対策	6.3	C		(e) 機器を用いる場合は機器の管理	7.6.13	アクセス制御方針	実施すべき安全管理策	(1)情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること (2)情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること
	(ウ)6	組織的安全管理対策	6.3	C		(f) 個人情報の記録媒体の管理(保管・授受等)の方法	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(2)情報交換手順では搬送の形態によらず次の事項を確実にすること。 ●交換する情報の機密レベルに関して合意すること(受領側で機密レベルが低くならないこと)。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）7	組織的安全管理対策	6.3	C		(g) 患者等への説明と同意を得る方法				
	（ウ）8	組織的安全管理対策	6.3	C		(h) 監査	7.6.12	ログの取得及び監査	推奨される安全管理策	(1)監査ログに記録する事項としては次のようなものが考えられる。 ●作業者情報(作業者ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元IPアドレス) ●ファイル及びデータへのアクセス、変更、除記録(作業者ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類) ●データベース操作記録(作業者ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元IPアドレス、設定変更時にはその内容) ●修正パッチの適用作業(作業者ID、変更されたファイル) ●特権操作(特権取得者ID、特権取得の可否、利用時刻及び時間、実行作業内容) ●システム起動、停止イベント ●ログ取得機能の開始、終了イベント ●外部デバイスの取り外し ●IDS・IPS等のセキュリティ装置のイベントログ ●サービス及びアプリケーションの動作により生成されたログ(時刻同期に関するログを含む)
	（ウ）9	組織的安全管理対策	6.3	C		(i) 苦情・質問の受け付け窓口				
	（エ）1	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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(6)サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	(エ)2	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。				
	(エ)3	組織的安全管理対策	6.3			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。				
3.2.2		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。	7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項②	実施すべき安全管理策	(2)医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。 (3)情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。
							7.5.1	医療情報処理施設の建物に関する要求事項	実施すべき安全管理策	(1)情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ 環境(専有サーバ、仮想プライベートサーバ等)を利用する場合においても、同等の措置がとられていることを確認すること。 ●医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。
							7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項②	推奨される安全管理策	(1)医療情報システムの設置されるサーバラックの施錠装置については、ハードウェアトークン又はICカード等の認証デバイス、暗証番号(PIN)、パスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせることが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）1						7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項③	実施すべき安全管理策	サーバ環境を運営する外部事業者が、①及び②と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。
		保存性の確保	7.3	D		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）2	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。				
		保存性の確保	7.3	C		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。				
		保存性の確保	7.3	D		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。				
	（ア）3					明文規定なし	7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(5)火災発生時の消火設備が機器に損傷を与えないよう配慮すること。 (6)医療情報システムを配置する室内での喫煙、飲食を禁止すること。 (7)医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。 (10)医療情報システムを設置するサーバラックについては以下の安全管理策を実施すること。 ●震災時に転倒することが無いよう確実に設置すること。 ●熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。 ●扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。
							7.5.1	医療情報処理施設の建物に関する要求事項	実施すべき安全管理策	(1)情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境(専有サーバ、仮想プライベートサーバ等)を利用する場合においても、同等の措置がとられていることを確認すること。 ●自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）1	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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(5)サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。 (6)サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。
							7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項①	実施すべき安全管理策	(1)医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。 (2)有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。 (3)有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること(履歴の保全については「7.6.12ログの取得及び監査」を参照)。 (4)情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。 (5)情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。 (6)職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、情報処理事業者職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行うこと。 (7)情報処理事業者の職員の業務に応じて執務室内に滞在できる時間を指定すること。 (8)医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(4)医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。
							7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項①	推奨される安全管理策	機械式の認証装置で利用する認証要素としては、ハードウェアトークン又はICカード等の認証デバイス、暗証番号(PIN)、パスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせることが望ましい。
							7.5.2	医療情報処理施設への入退館、入退室等に関する要求事項③	実施すべき安全管理策	サーバ環境を運営する外部事業者が、①及び②と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）2	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。	7.5.1	医療情報処理施設の建物に関する要求事項	実施すべき安全管理策	(1)情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ 環境(専有サーバ、仮想プライベートサーバ等)を利用する場合においても、同等の措置がとられていることを確認すること。 ●傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。
		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）1	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。	7.5.1	医療情報処理施設の建物に関する要求事項	実施すべき安全管理策	(1)情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ 環境(専有サーバ、仮想プライベートサーバ等)を利用する場合においても、同等の措置がとられていることを確認すること。 ●傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。
		人的安全管理対策	6.6	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。				
	（エ）1	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。				
3.2.3							7.6.10	アプリケーションに対するセキュリティ要求事項	実施すべき安全管理策	(3)アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。 (4)アプリケーションにて医療事業者側の作業者を認証する情報(ID/パスワード認証の際のパスワード)は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。
							7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	(10) 医療情報システムのサーバ機器等への同時ログオンユーザ数(OSアカウント等)に適切な上限を設けること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）1	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	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(4)サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。
							7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて推奨される安全管理策	（1）不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。
							7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて推奨される安全管理策	(3)認可されていない作業者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると作業者IDが存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）2	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。	7.6.15	作業者の責任及び周知	実施すべき安全管理策	（1）各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。 （2）システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。
							7.6.14	作業者アクセス及び作業者IDの管理	パスワード管理について実施すべき安全管理策	(6)パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。 (8)パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。
							7.6.14	作業者アクセス及び作業者IDの管理	パスワード管理について推奨される安全管理策	(2)パスワードの品質基準としては、パスワードを十分に長くすること(8文字以上等)、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。
		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。	7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて実施すべき安全管理策	（2）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こと。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）3	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。	7.6.14	作業者アクセス及び作業者IDの管理	パスワード管理について実施すべき安全管理策	(1)情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。 (2)医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。 (3)医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。 (4)医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。 (7)パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。 (9)パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。
							7.6.14	作業者アクセス及び作業者IDの管理	パスワード管理について推奨される安全管理策	(1)作業者が医療情報システムへのログオン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。 (2)パスワードの品質基準としては、パスワードを十分に長くすること(8文字以上等)、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。
							7.6.14	作業者アクセス及び作業者IDの管理	パスワード管理について実施すべき安全管理策	(5）パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。
	（ア）4	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。				
		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。	7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて推奨される安全管理策	(5)ログオン時に利用する認証要素としては、ハードウェアトークン又はICカード等の認証デバイス、暗証番号(PIN)、パスワード等の記憶要素、生体情報(バイオメトリクス)等を組み合わせることが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）1	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。	7.2.2	情報の分類	実施すべき安全管理策	(1)情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。 (2)情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。 (3)預託される情報に対して分類にもとついたリスク分析を実施すること。 (4)リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。 (5)分類がわかるように情報にラベルをつけること(電磁的記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること)。 (6)各ラベルに応じた処理方式(保存、配送、複製、廃棄等)を定めること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
							7.7	人的安全対策	実施すべき安全管理策安全管理措置	(3)情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。
	(イ)2	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。	7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて推奨される安全管理策	(2)不正なアカウントの利用を防ぐため、作業者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。
							7.6.13	アクセス制御方針	実施すべき安全管理策	(3)アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。 (4)それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。 (5)業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。
							7.6.13	アクセス制御方針	推奨される安全管理策	80
							7.6.10	アプリケーションに対するセキュリティ要求事項	実施すべき安全管理策	(5)アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。
	(イ)3	見読性の確保	7.2	C	【保存する場所について共通する内	(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	(ウ)	真正性の確保	7.1		基本的事項	(1)入力者及び確定者の識別及び認証				
	(ウ)(a)	真正性の確保	7.1			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)入力者及び確定者の識別及び認証				
		真正性の確保	7.1	C	a. 電子カルテシステム等で	1. 入力者及び確定者を正しく識別し、認証を行うこと。	7.6.10	アプリケーションに対するセキュリティ要求事項	実施すべき安全管理策	(3)アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。 (4)アプリケーションにて医療事業者側の作業者を認証する情報(ID/パスワード認証の際のパスワード)は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）(a)1	真正性の確保	7.1	C	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。	7.6.10	アプリケーションに対するセキュリティ要求事項	実施すべき安全管理策	(5)アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。
		真正性の確保	7.1	C		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	(ウ)(a)2	真正性の確保	7.1	C	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	b-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。				
		真正性の確保	7.1	C		b-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。				
	(ウ)(b)2	真正性の確保	7.1	C		(2) 記録の確定手順の確立と、作成責任者の識別情報の記録				
	(ウ)(b)1	真正性の確保	7.1	C	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、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が含まれること。				
		真正性の確保	7.1	C		2. 「記録の確定」を行うに当たり、内容の十分な確認が実施できるようにすること。				
		真正性の確保	7.1	C		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。				
		真正性の確保	7.1	C		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、また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		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。				
		真正性の確保	7.1	C		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
		真正性の確保	7.1	C	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. 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、当該装置の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. 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。				
	（ウ）(c)	真正性の確保	7.1	C		（3）更新履歴の保存				
		真正性の確保	7.1	C		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。				
		真正性の確保	7.1	C		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。				
	（ウ）(d)	真正性の確保	7.1	C		（4）代行入力の承認機能				
		真正性の確保	7.1	C		1. 代行入力を実施する場合、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。				
		真正性の確保	7.1	C		2. 代行入力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。				
		真正性の確保	7.1	C		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.3	（エ）1	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。	7.6.12	ログの取得及び監査	実施すべき安全管理策	（1）作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。 （2）監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。
							7.6.12	ログの取得及び監査	推奨される安全管理策	(1)監査ログに記録する事項としては次のようなものが考えられる。 ●作業者情報(作業者ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元IPアドレス) ●ファイル及びデータへのアクセス、変更、除記録(作業者ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類) ●データベース操作記録(作業者ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元IPアドレス、設定変更時にはその内容) ●修正パッチの適用作業(作業者ID、変更されたファイル) ●特権操作(特権取得者ID、特権取得の可否、利用時刻及び時間、実行作業内容) ●システム起動、停止イベント ●ログ取得機能の開始、終了イベント ●外部デバイスの取り外し ●IDS・IPS等のセキュリティ装置のイベントログ ●サービス及びアプリケーションの動作により生成されたログ(時刻同期に関するログを含む) (3)監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者IDと、情報の識別子(資産台帳記載の番号等)、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。 ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサ-バにログデ-タを集約して分析管理することが望ましい。
							7.6.9	医療情報システムに対するセキュリティ要求事項	実施すべき安全管理策	(4)運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。 (5)システム運用情報(システム及びサービス設定ファイル等)の複製及び利用については監査証跡とするためにログを取得すること。
							7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	(11)ネットワーク接続のログ(認証ログ及び接続ログ)を記録すること。 (12)ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。
		保存性の確保	7.3	C		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。	7.2.2	情報の分類	推奨される安全管理策	情報の処理について履歴を取得し、資産台帳等に記録することが望ましい。
	（エ）2	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。	7.6.12	ログの取得及び監査	実施すべき安全管理策	(5)ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。 ●ログデータにアクセスする作業者及び操作を制限すること。 ●容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。 ●ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（エ）3	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。	7.6.12	ログの取得及び監査	実施すべき安全管理策	(3)ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。 （4）標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。
							7.6.12	ログの取得及び監査	推奨される安全管理策	(1)医療情報システムのすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（オ）1	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。	7.6.15	作業者の責任及び周知	実施すべき安全管理策	（3）離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。
		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）。	7.6.15	作業者の責任及び周知	実施すべき安全管理策	（3）離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。
	（オ）1	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。	7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて実施すべき安全管理策	（1）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、作業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、あるいは強制ログオフを行うこと。
	（カ）1	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(2)情報交換手順では搬送の形態によらず次の事項を確実にすること。 ●交換された情報に悪意のあるコードが含まれていないことを確実とすること。
							7.6.3	悪意のあるコードに対する管理策	実施すべき安全管理策	(1)最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス(ワーム)、バックドア(トロイの木馬)、スパイウェア(キーロガー)、ボットプログラム(ダウンローダー)等がある。 (2)悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ●リアルタイムスキャン(ディスク書き出し・読み込み、ネットワーク通信) ●リスク評価の結果として必要であれば定期的にスキャンを実施 ●電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン ●定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ●管理者以外による設定変更やアンインストールの禁止 (3)一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
							7.5.4	情報処理装置の廃棄及び再利用に関する要求事項	実施すべき安全管理策安全管理措置	(3)ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。
		保存性の確保	7.3		基本的事項	(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				
		保存性の確保	7.3	C		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（カ）2	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。	7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	(1)セキュリティゲートェイ(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こと。ホスティング利用時等、ネットワーク境界にセキュリティゲートェイを設置できない場合は、個々の情報処理装置(サーバ)にて、同様のアクセス制御を行うこと。 (2)セキュリティゲートェイでは、不正なIPアドレスを持つトラフィックが通過できないように設定すること(接続機器類のIPアドレスをプライベートアドレスとして設定して、ファイアウォール、VPN装置等のセキュリティゲートウェイを通過しようとするトラフィックをIPアドレスベースで制御する等)。 (5)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の検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、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、同様の制御を行うこと。 (6)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こと。 (7)侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。 (8)侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。
							7.6.6	ネットワークセキュリティ管理	推奨される安全管理策	(1)医療情報システムから、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。 (2)侵入検知システム自身が攻撃・不正アクセスの対象とならないように、その存在を 外部から隠す設定(ステルスモード)や、侵入検知システムへのアクセスの適切な制御を実施することが望ましい。
							7.6.7	電子媒体の取扱	推奨される安全管理策	(2)医療情報システムにおいてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除することが望ましい。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。 (3)不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(13)不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。

総務省クラウドサービス医療情報ガイドライン(案)		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	(キ)	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。				
	(ク)1	保存性の確保	7.3	C		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。				
	(ク)2	保存性の確保	7.3	D		(3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止 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。				
	(ク)2	保存性の確保	7.3	C		(3) 記録媒体、設備の劣化による読み取り不能また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。	7.6.7	電子媒体の取扱	実施すべき安全管理策	(6)製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ク）3	見読性の確保	7.2	C		（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。	7.10.1	要求事項の識別	実施すべき安全管理策	（6） ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG及びPNG 等のフォーマット46）で外部ファイルに出力可能とすることなどの方策を検討すること。
		保存性の確保	7.3	D		1. 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。	7.6.7	電子媒体の取扱	実施すべき安全管理策	(7)情報を保管するためにハードディスク装置を用いる場合には、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。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(12)情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。
	（ク）4	保存性の確保	7.3	C		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。				
	（ク）5	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	（ケ）1	真正性の確保	7.1	C		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。				
	（ケ）1	真正性の確保				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。	7.9	医療情報システムの改造と保守	推奨される安全管理策	(1) 開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。 パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的なぜい弱性検査を行う。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(2)医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。 (8)それぞれの装置は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。
	（ケ）2	真正性の確保	7.1	C		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。	7.6.10	アプリケーションに対するセキュリティ要求事項	実施すべき安全管理策	(1)提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。 (2)アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア(ライブラリ、サーバプロセス等)については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ケ）2	真正性の確保	7.1	C		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。	7.6.9	医療情報システムに対するセキュリティ要求事項	実施すべき安全管理策	(5)システム運用情報(システム及びサービス設定ファイル等)の複製及び利用については監査証跡とするためにログを取得すること。
							7.6.1	情報処理装置及びソフトウェアの保守	実施すべき安全管理策	(6)不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査(改ざん検知)を実施すること。 (7)医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。
3.2.3	（コ）1.	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。	7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	医療情報を保存する医療情報システムにおいて無線ネットワーク(Bluetooth等の近距離無線通信を含む)LANを利用しないこと。
3.2.3	（コ）2	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。				
		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。				
		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。	7.6.9	医療情報システムに対するセキュリティ要求事項	実施すべき安全管理策	(4)運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。 (5)システム運用情報(システム及びサービス設定ファイル等)の複製及び利用については監査証跡とするためにログを取得すること。
		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.4	（ア）1	人的安全管理対策	6.6	C	（ア）従業者に対する人的安全管理措置	1-① 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。	7.7	人的安全対策	実施すべき安全管理策安全管理措置	（1）医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。 (5)医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。
							7.7	人的安全対策	推奨される安全管理策	（1）医療情報を操作する情報処理事業者職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これは服務規程等に含めることもできる。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行うこと。
		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。				
	（ア）2	人的安全管理対策	6.6	C	（ア）従業者に対する人的安全管理措置	1-② 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。	7.7	人的安全対策	実施すべき安全管理策安全管理措置	（2）医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。
	（ア）3	人的安全管理対策	6.6	C	（ア）従業者に対する人的安全管理措置	1-③ 従業者の退職後の個人情報保護規程を定めること。	7.7	人的安全対策	実施すべき安全管理策安全管理措置	(4)医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。
	（ア）4	人的安全管理対策	6.6	C		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。				
		人的安全管理対策	6.6	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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	(ア)5	人的安全管理対策	6.6	C	（ア）従業者に対する人的安全管理措置	1．医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。				
	(イ)1	人的安全管理対策	6.6	C		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。				
		人的安全管理対策	6.6	C		④ 委託事業者が再委託を行うか否かを明確にし、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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(1)第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。 (2)サービスの実施、運用、維持について定期的に検証すること。 (3)サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。
							7.6.5	第三者が提供するサービスの管理	推奨される安全管理策	(1)外部事業者がサービスを実施する際は、情報処理事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。
3.2.5	(ア)1	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。	7.8	情報の破棄	実施すべき安全管理策	（1）CD-R等の廃棄については「7.6.7電子媒体の取扱」を参照すること。 （2）ハードディスク等の廃棄については「7.5.4情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。
							7.6.7	電子媒体の取扱	実施すべき安全管理策	(1)電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。CD、DVD、MO等の電子媒体については、追記のできない光学メディア(CD-R、DVD-R等)を用い、情報交換作業終了後、電子媒体を(9)に示す方式にて確実に廃棄処分すること。
							7.6.7	電子媒体の取扱	推奨される安全管理策	(1)物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）1	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。	7.8	情報の破棄	実施すべき安全管理策安全管理措置	（3）情報処理事業者は医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出すること。
							7.5.4	情報処理装置の廃棄及び再利用に関する要求事項	実施すべき安全管理策安全管理措置	(4)ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置(高温による融解、裁断等)等を適用し、当該装置に実施した措置の概要の記録(対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等)について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。
							7.5.4	情報処理装置の廃棄及び再利用に関する要求事項	推奨される安全管理策	(1)物理的な破壊措置については情報処理事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておくこと。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。
	（ア）2	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。				
		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	7.6.7	電子媒体の取扱	推奨される安全管理策	(1)物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）1	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。	7.6.14	作業者アクセス及び作業者IDの管理	特権IDについて実施すべき安全管理策	(1)特権IDの発行は必要な最小限のものに留めること。 (2)特権使用者に昇格可能な作業者IDを制限すること。 (3)特権の使用時には作業実施内容を記録すること。
							7.6.14	作業者アクセス及び作業者IDの管理	特権IDについて推奨される安全管理策	(1)特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。 (2)システムの機能として可能であれば、特権IDで使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。
							7.6.14	作業者アクセス及び作業者IDの管理	作業者IDについて実施すべき安全管理策	(1) 作業者は情報処理装置上においてユニークな作業者ID により識別されること。 (2) 作業者ID を発行する際に、既存のID との重複を排除する仕組みを導入すること。 (3) 複数作業者で共用するためのグループID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者ID でログオンしてからグループID に変更する仕組みを利用すること。 (4) 作業者ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。 (5) 作業者が変更あるいは退職した際には、ただちに当該作業者ID を利用停止とすること。 (6) 監視ログの監査時に作業者を確実に特定するため、作業者ID は過去に使われたものを再利用しないこと。 (7) 不要な作業者ID が残っていないことを定期的に確認すること。
							7.6.14	作業者アクセス及び作業者IDの管理	作業者IDについて推奨される安全管理策	(1)アクセスを許可された作業者IDのアクセス可能範囲が許可された通りとなっていること(不正に変更されていないこと)を定期的に確認することが望ましい。
	（ア）2	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。	7.6.14	作業者アクセス及び作業者IDの管理	特権IDについて実施すべき安全管理策	(4)管理端末以外からの特権IDによる直接ログオンを禁止すること。
							7.6.14	作業者アクセス及び作業者IDの管理	作業者IDについて実施すべき安全管理策	(4)作業者IDの発行は医療情報システムの管理に必要な最小限の人数に留めること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）1	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。				
		真正性の確保	7.1	C		（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。				
		人的安全管理対策	6.6	C		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・作業結果の確認をおこなうこと。				
	（イ）2	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。	7.6.9	医療情報システムに対するセキュリティ要求事項	実施すべき安全管理策	(4)運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。 (5)システム運用情報(システム及びサービス設定ファイル等)の複製及び利用については監査証跡とするためにログを取得すること。
		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。				
	（イ）3	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。				
	（イ）4	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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(3)サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。
							7.6.1	情報処理装置及びソフトウェアの保守	実施すべき安全管理策	(4)情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。 (5)情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）1	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。	7.6.10	アプリケーションに対するセキュリティ要求事項	推奨される安全管理策	(1)アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。
							7.6.9	医療情報システムに対するセキュリティ要求事項	実施すべき安全管理策	(1)運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類を運用システム上に置かないこと。 (2)情報処理に不必要なファイル等を運用システム上におかないこと。
							7.6.2	開発施設、試験施設と運用施設の分離	実施すべき安全管理策	(5)運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。 (6)医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用すること。
	（ウ）2	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。				
		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。				
	（エ）1	保存性の確保				（4） 媒体・機器・ソフトウェアの整合性不備による復元不能の防止				
		保存性の確保	7.3	C		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。				
	（エ）2	保存性の確保	7.3	C		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		保存性の確保			医療機関等以外に保存する際の要求事項	（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				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（エ）3	保存性の確保	7.3	C		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。	7.6.1	情報処理装置及びソフトウェアの保守	実施すべき安全管理策	(1) オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。 (3)医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する問、以前のデータ形式、プロトコルの利用をサポートすること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
		保存性の確保	7.3			（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				
	（エ）4	保存性の確保	7.3	C		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。				
	（エ）5	保存性の確保	7.3	C		（3）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	（オ）1	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。				
	（オ）2	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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	(1)第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。 (8)医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第4.1版」6.8章C項の管理策を実施すること。
3.2.7	（ア）1	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(3)物理的に情報を搬送する際には以下の対策を実施すること。 ●医療機関等が合意する基準にもとついて信頼できる配送業者を選択すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）2	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(3)物理的に情報を搬送する際には以下の対策を実施すること。 ●配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。 ●配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。 ●配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。 ●電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
							7.5.5	情報処理装置の外部への持ち出しに関する要求事項	実施すべき安全管理策	(1)情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。 (2)持ち出した機器を再度設置するための適切な検証手順を策定すること。
							7.5.5	情報処理装置の外部への持ち出しに関する要求事項	推奨される安全管理策	(1)持ち出し手順に含まれる事項には次のようなものが考えられる。 ●装置の持ち出し申請書のフォーマット(申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ●申請承認プロセス ●返却確認プロセス、等。 (2)返却時の検証手順に含まれる事項には次のようなものが考えられる。 ●装置の動作確認 ●盗聴装置等、情報の安全性を脅かす装置の有無 ●悪意のあるプログラムの検出作業 ●収められている情報の検証作業(不正な改ざん等)、等。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(9)保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択すること。
		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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
		保存性の確保	7.3	C		(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。				
	(ア)3	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。				
	(ア)4	情報および情報機器の持ち出し	6.9			6.9全般				
3.2.7	(イ)	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。	7.6.7	電子媒体の取扱	実施すべき安全管理策	(2)情報交換目的やバックアップ目的でMT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。 (3)電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。 (4)電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。
							7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(1)不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.7	（ウ）1	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。	7.5.3	情報処理装置のセキュリティ	実施すべき安全管理策	(11)起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「7.6.14作業者アクセス及び作業者IDの管理」に従うこと。
		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。				
	（ウ）2	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(3)物理的に情報を搬送する際には以下の対策を実施すること。 ●電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。
	（ウ）3	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。				
	（ウ）4	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。				
		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）5	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。				
3.2.8	（ア）1	見読性の確保	7.2	C		（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）2	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。				
	（ア）3	見読性の確保	7.2	C		（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。	7.10.1	要求事項の識別	実施すべき安全管理策	(6) ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG及びPNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を検討すること

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）4	見読性の確保	7.2	C		（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。	7.10.1	要求事項の識別	実施すべき安全管理策	（7） 医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ア）5	見読性の確保	7.2		【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				
		見読性の確保	7.2	C		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	（イ）1	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。	7.10.2	事業継続計画の立案及びレビュー	実施すべき安全管理策	（1） 医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画を策定すること。 （2） 策定した事業継続計画について模擬試験を含めた適切な方法でレビューすること。 （3） 事業継続計画について定期的に見直しを行うこと。
							7.10.2	事業継続計画の立案及びレビュー	推奨される安全管理策	（1） 策定される事業継続計画には次のような事項を含むことが望ましい。 事前準備計画 「非常時」判断手順 関係者の召集、対応本部の設置 機器及び作業員の縮退措置及び代替施設の手配措置 バックアップ施設等、代替施設への切替え措置 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） 障害の拡大範囲に関する判断手順、基準
	（イ）2	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。	7.10.2	事業継続計画の立案及びレビュー	推奨される安全管理策	（1） 策定される事業継続計画には次のような事項を含むことが望ましい。 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） 正常復帰の判断手順、基準 正常復帰後の医療情報システムの点検手順（不正侵入、情報改ざん、情報破損等の検出等）
	（イ）3	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。	7.6.14	作業者アクセス及び作業者IDの管理	作業者のログオンについて推奨される安全管理策	(4)緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）4	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）	7.10.2	事業継続計画の立案及びレビュー	推奨される安全管理策	所管官庁への連絡体制、等

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.9	（ア）1	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(4) 電子的に情報を転送する際には以下の対策を実施すること。 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。 認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 送受信する経路は適切な方法で傍受のリスクから保護されていること。 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。
							7.6.4	ウェブブラウザを使用する際の要求事項	実施すべき安全管理策	(1)ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること (2)ウェブブラウザの設定で、認可していないサイトから、ActiveX、Javaアプレット、Flash等のプログラムコードをダウンロード及び実行することができない設定になっていること(管理ソフトウェアが実行されるサーバのみを認可する)。 (3)認可したサイトからダウンロードされるコードについても「7.6.3悪意のあるコードに対する管理策」に即して検査されること。
							7.6.4	ウェブブラウザを使用する際の要求事項	推奨される安全管理策	(1)ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。
							7.5.3	情報処理装置のセキュリティ	推奨される安全管理策	(1)情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.9	（ア）2	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(4) 電子的に情報を転送する際には以下の対策を実施すること。 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。
							7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(2)情報交換手順では搬送の形態によらず次の事項を確実にすること。 ●発送者、受領者を識別し記録すること。 ●発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行うこと。 (4)電子的に情報を転送する際には以下の対策を実施すること。 ●送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。 認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。
		真正性の確保	7.1	C	医療機関等以外に保存する際の要求事項（厚生労働省ガイドラインでは【ネットワークを通じて医療機関等の外部に保存する場合】に記述）	（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行うこと 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、お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。				
	（ア）3	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。	7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	(3)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。 (4)ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。 (14)VPN接続を行う場合には以下の事項に従うこと。 ●接続時にVPN装置間で相互に認証を行うこと。 ●傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11暗号による管理策」に従い、適切な暗号技術を利用すること。 ●インターネット上のトラフィックがVPNチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。 ●複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPNチャンネルを医療機関等別に構築する等の対策を実施すること。
							7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(4) 電子的に情報を転送する際には以下の対策を実施すること。 認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）1	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。	7.6.11	暗号による管理策	実施すべき安全管理策	(1)暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト42等を用いること。 (2)暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。 (3)電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。 (4)暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。 (5)医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。
							7.6.11	暗号による管理策	推奨される安全管理策	(1)暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。 (2)暗号鍵の生成は耐タンパー性44を有するICカード、USBトークンデバイスといった安全な環境で実施することが望ましい。 (3)暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。
							7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(4)電子的に情報を転送する際には以下の対策を実施すること。 ●受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。 ●送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。
		真正性の確保	7.1	C		（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・解凍並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。				
	（イ）2	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。	7.6.6	ネットワークセキュリティ管理	実施すべき安全管理策	(9)医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。 ●外部からの医療情報システムの稼働監視・遠隔保守 ●セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ●オペレーティングシステム及び利用アプリケーションのセキュリティパッチ ファイル等のダウンロード ●電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ●ファイアウォール、IDS・IPSなどのセキュリティ機器に対する不正アクセス監視 ●時刻同期のための時刻配信サーバへのアクセス ●これらのサービスを利用するために必要なインターネットサービス(ドメインネームサーバへのアクセス等) ●その他の医療情報システムの稼動に必要なサービス(外部認証サーバ、外部医療情報データベース等)

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）3	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。				
	（イ）4	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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）1	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。				
	（エ）1	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）。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(1)次の情報交換方法について予め合意しておくこと。 ●情報を電子媒体に記録して交換する際の手順 ●情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ●情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ●情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順
3.2.9	（エ）2	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、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。	7.6.4	ウェブブラウザを使用する際の要求事項	実施すべき安全管理策	(1)ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること (2)ウェブブラウザの設定で、認可していないサイトから、ActiveX、Javaアプレット、Flash等のプログラムコードをダウンロード及び実行することができない設定になっていること(管理ソフトウェアが実行されるサーバのみを認可する)。 (3)認可したサイトからダウンロードされるコードについても「7.6.3悪意のあるコードに対する管理等に即して検査されること
							7.6.4	ウェブブラウザを使用する際の要求事項	推奨される安全管理策	(1)ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。
		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	8.1.2	C		(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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.2.10	（ア）	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				
		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. 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。				
	（ア）	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。	7.6.11	暗号による管理策	実施すべき安全管理策	(3)電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。
							7.6.11	暗号による管理策	推奨される安全管理策	(3) 暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。 (4)電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望ましい。
							7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(1) 次の情報交換方法について予め合意しておくこと。 ●情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順
		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.「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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(1) 次の情報交換方法について予め合意しておくこと。 ●情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順
	（イ）	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。	7.6.8	情報交換に関するセキュリティ	実施すべき安全管理策	(1) 次の情報交換方法について予め合意しておくこと。 ●情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順
	（イ）	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. 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。				
	（イ）	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. 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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（ウ）	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。	7.6.11	暗号による管理策	実施すべき安全管理策	(3)電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。 （4）暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。 （5）医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.3.6	（ア）	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		(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。少なくとも以下の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	7.3	組織的安全管理策(体制、運用管理規程)	実施すべき安全管理策	(1)医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。 (2)個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
							7.1.1	ISMS認証取得時の考慮事項	推奨される安全管理策	(1)認証取得あるいは更新の際にISMSの安全管理策として、本ガイドライン「7医療情報を受託管理する情報処理事業者における安全管理上の要求事項」にて提示する安全管理策を盛り込むことが望ましい。 (2)受託管理する医療情報の入り口から出口まで包括的にISMSの適用範囲とすることが望ましい。 (3)安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくことが望ましい(適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること)。

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
	（イ）1	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		(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。				
		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。				
	（イ）2	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。				
	（ウ）1	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		(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。				
	（ウ）2	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		(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。				

総務省クラウドサービス医療情報ガイドライン（案）		厚生労働省ガイドライン					経産省医療ガイドライン			
項番	サブ項番	項目	節	記載箇所	小項目	記載内容	節	節タイトル	記載箇所	記載内容
3.3.7	（ア）	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。	7.3	組織的安全管理策（体制、運用管理規程）	実施すべき安全管理策	⑶個人情報保護に関しては、医療機関等の監督の下に行うこと。
3.3.7	（イ）	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。				
3.4		個人情報の保護	8.4.2	C		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。	7.6.5	第三者が提供するサービスの管理	実施すべき安全管理策	⑺サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。