参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
6 情報システムの基本的な安全管理					
	6.1 方針の制定と公表				
	少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること				
	6.2 情報の取扱いの把握とリスク分析				
	6.2.1 取扱い情報の把握				
	情報システムで扱う情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある				
	このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理されなければならない				
	医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類する				
	6.2.2 リスク分析				
	分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する				
	説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある				
	に安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない				
	医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある				
	6.3 組織的安全管理対策（体制、運用管理規程）				
	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				
	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. 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				
	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				
	5. 運用管理規程等において次の内容を定めること (a) 個人情報の記録媒体の管理（保管・授受等）の方法 (b) リスクに対する予防、発生時の対応の方法				
	6.4 物理的安全対策				
	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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	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、権限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、本体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. 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。 ・ 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こと。 ・ 入退者の記録を定期的にチェックし、妥当性を確認すること				
	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				
	5. 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること				
	（以下、推奨されるガイドライン）				
	防犯カメラ、自動侵入監視装置等を設置すること				
	6.5 技術的安全対策				
	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				
	2. 動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意すること				
	3. 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。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、現状でそのような機能がない場合は、システム更新までの期間、運用管理規定でアクセス可能範囲をさだめ、次項の操作記録を行なうことで担保する必要がある				
	4. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録はすくなくとも利用者のログイン時刻および時間、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）を必ず行うこと				
	5. 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				
	6. システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認すること				
	7. 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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	(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(不可逆)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)、極端に短い文字列を使用しないこと(8 バイト以上の可変長の文字列が望ましい)。				
	(2) 類推しやすい、不注意によるパスワードの盗用は、盗用された本人の責任になることを認識すること				
	(以下、推奨されるガイドライン)				
	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること				
	2. アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと				
	3. 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(たとえばパターンファイルの更新の確認・維持)を行なうこと				
	4. 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)				
	5. 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)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				
	6. 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. 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が望ましい。				
	6.6 人的安全対策				
	(1) 従業者に対する人的安全管理措置				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	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				
	2. 定期的に従業者に対し教育訓練を行うこと				
	3. 従業者の退職後の個人情報保護規程を定めること				
	（以下、推奨されるガイドライン）				
	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				
	(2) 事務取扱委託業者の監督及び守秘義務契約				
	1. 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、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、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 包括的な委託先の罰則を定めた就業規則等で裏づ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・作業結果の確認をおこなうこと。				
	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 委託先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先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				
	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づけられた守秘契約等の秘密保持の対策を行うこと				
	6.7 情報の破棄				
	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				
	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. 破棄を外部事業者に委託した場合は、「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、さらに委託元の医療機関等が確実に情報の破棄が行なわれたことを確認すること				
	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廃棄を定める規程の作成の方法				
	6.8 情報システムの改造と保守				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	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				
	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、およ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. 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				
	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				
	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				
	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				
	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				
	8. リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること				
	9. 再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。				
	（以下、推奨されるガイドライン）				
	1. 詳細なオペレーション記録を保守操作ログとして記録すること				
	2. 保守作業時には病院関係者立会いのもとで行うこと				
	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				
	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				
	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				
	6.9 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				
	① 秘匿性の確保のための適切な暗号化				
	電気通信回線を塚する際の個人情報保護は、通信手段の種類によって個別に考える必要がある。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。				
	電気通信回線を通貨する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。				
	② 通信の起点・終点識別のための認証				
	起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の機関と受託先の機関を確実に相互に認証しなければならない。				
	③ リモートログイン制限機能				
	個人情報を含む医療情報の保存業務を受託先の機関や委託元の機関のサーバへのリモートログイン機能に制限を設けないで容認すると、ログインのためのパスワードが平文でLAN回線上に流れたり、ファイル転送プログラム中にパスワードがそのままの形でとりこまれたりすることにより、これが漏洩する可能性がある。				
	認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。				
	一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。				
	リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。適切に管理されたリモートログイン機能のみに制限しなければならない。				
7 電子保存の要求事項について					
	7.1 真正性の確保について				
	(1) 作成者の識別及び認証				
	a. 電子カルテシステム等、PC 等の汎用入力端末により記録が作成される場合				
	1. 利用者にID、パスワード等の本人認証、識別に用いる識別情報を発行し、本人しか持ち得ない、または知り得ないように運用を定めること。システムは発行されたID、パスワード等による本人認証、識別機能を有すること。ただし、運用により確実に担保される場合は除く				
	2. 本人認証、識別にIC カード等のセキュリティ･デバイスを利用する場合は、そのデバイス単独で有効にならないようにし、必ずユーザID やパスワードと組み合わせた識別、認証を行うこと				
	3. 本人認証、識別に指紋、虹彩等のバイオメトリクスを利用する場合は、1 対1 の照合となるよう、必ずユーザID やパスワードと組み合わせた識別、認証を行うこと				
	4. 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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	5. 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。				
	6. 情報システムに医療機関等外からリモート接続する場合は、暗号化、ネットワーク接続端末のアクセス制限等のセキュリティ対策を実施すること				
	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				
	装置の管理責任者や操作者が運営管理規程で明文化され、管理責任者、操作者以外の機器の操作が運営上防止されていること				
	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営の組み合わせにより明確になっていること				
	(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				
	a. 電子カルテシステム等、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が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。				
	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. 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を運用も含めて防止でき、それらが検知された場合はバックアップ等を用いて原状回復できるようになっていること				
	4. 外部から入力された情報を「参照」する場合、その情報は本ガイドラインに従って正しく保存された確定記録でなければならない				
	参照元の情報が「保存された記録」でない場合は、コピー等の移動手段を経て取り込み操作を行った後に、その情報も含めた「記録の確定」が行われなければならない				
	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				
	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）、信頼できる時間源を用いた作成日時が記録に含まれること				
	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を運用も含めて防止でき、それらが検知された場合はバックアップ等を用いて原状回復できるようになっていること				
	(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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	2. 更新履歴の参照(照らし合せ)は、更新前後の情報が各々物理的に独立して保存されているものの様に更新の順序に沿って参照する方法か、更新時の変更点を明示するような方法(消し込み線を表示するように)で参照できること				
	3. 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				
	4. アクセスログの記録を残し、そのログが改ざんされない対策を講じ、万が一、記録情報の改ざん・削除が起こった場合にはその事実を検証可能とすること。				
	(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、具体的にどの医療に関する業務等(プロシジャ)に適用するか、また誰が誰を代行してよいかを定義すること				
	2. 代行操作を認める医療に関する業務等がある場合は、その代行操作者自身も予め電子保存システムの運用操作に携わる者として当該システムに識別管理情報を登録すること				
	3. 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				
	4. 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作成責任者による「確定操作(承認)」が行われること				
	このため、代行入力により記録された情報及びその管理情報は必要な都度参照ができるとともに、一定の期間内に確定操作が行われるように督促機能が組織のルールとして整備されていること				
	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、作成責任者を特定する明確なルールを策定し運用規程に明記すること				
	(5) 1 つの診療録等を複数の医療従事者が共同して作成する場合の管理				
	1. 診療録等を共同して作成するケースが運用上あれば、具体的にどの医療に関する業務等に適用するか定義すること				
	それぞれを分担する役割者(ロール)を具体的な職種や所属部署等を用いて定義すること				
	2. それぞれの役割者による記述を(4)で定義された方法で代行するケースがあれば、それを分担する役割者を医療に関する業務等ごとに定義すること				
	3. 記述の分担単位に確定操作が行えるようになっており、それぞれの記述者の識別管理情報が記録されること				
	(6) 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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	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. 運用管理規程で決められた内容を遵守するために、従業者等への教育を実施すること				
	4. 内部監査を定期的に実施するこ				
	(7) ルールの遵守				
	1. 運用管理規程で決められた内容を遵守するためには、従業者等の教育とルールの徹底が重要である。教育とルールの遵守状況について常に状況を把握すること				
	2. ルールの改訂や新たな従業者等の登用の際には、教育を実施すること				
	3. ルールの遵守状況に関する内部監査を、定期的に(少なくとも半年に1 度)実施すること				
	(以下、推奨されるガイドライン)				
	(1) 作成・記録責任者の識別及び認証				
	1. 記録の作成入力に関与する利用者識別・認証用に電子証明書を発行し、本人しか持ち得ないよう私有鍵をIC カード等のセキュリティ・デバイスに格納する				
	2. 本人が私有鍵を活性化する際にはパスワードや生体認証等の認証情報を用い、その認証情報が暗号化されずにネットワークへ流れることのないような手段を用いること				
	電子証明書をシステムへの認証用に用いる際は少なくとも端末へのログオン毎に、電子署名用に用いる際には署名毎に私有鍵の活性化を求めること				
	3. 利用者の権限範囲に応じた適切なアクセスコントロール機能を有すること				
	4. 情報システムにリモートアクセスする場合には、VPN 等、通信経路の暗号化を実施するとともにIC カード、電子証明書とパスワード等、2 つ以上の要素からなる認証方式により利用者の識別、認証を求めること。				
	(2) 情報の確定手順の確立と、作成・記録責任の識別情報の記録				
	1. 「記録の確定」に際し、作成者責任者の電子署名を行うこと				
	確定操作がいつ行われたかを担保するために、確定操作後速やかに信頼できる時刻源を用いたタイムスタンプ署名を行うこと				
	2. 「記録の確定」に際し、その作成責任者の識別情報が電子署名により記録情報に関連付けられること				
	この際、署名はIC カード等のセキュアなトークン内で行われるか、利用者の端末内で行われる場合は署名後に私有鍵の情報が一切残らない方式を用いること				
	3. 電子署名は保存が義務づけられた期間より長期にわたり署名時点での証明書及び署名の有効性が確認できること				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	4. 「確定操作」を行うにあたり、責任者による内容の十分な確認が行われたことを確認する手続きを義務づけること				
	(3) 更新履歴の保存				
	1. 一旦確定された情報は、後からの追記・書き換え・消去等の事実を正しく確認できるよう、当該事項の履歴が保存され、その内容を容易に確認できること				
	追記・書き換え・消去等の確定操作を行う際には当該部分の変更履歴を含んだ電子署名をおこなうこと。				
	(4) 代行操作の承認機能(代行操作が運用上に必要な場合のみ)				
	1. 代行操作を認めるかどうかを医療に関する業務等(プロシジャ)ごとに定義しうること				
	2. 操作者の役割(ロール)を定義し、上記で定義したプロシジャに対して適用可否を判断できること				
	3. 代行操作が行われたプロシジャに対し、その承認者(作成責任者)による承認操作が行えること。また、その承認操作が督促されること				
	(5) 1 つの診療録等を複数の医療従事者が共同して作成する場合の管理				
	1. 1 つの診療録等に対し、複数の入力者による署名をサポートすること				
	この場合、1 つの情報単位に対して複数の署名を付与する実装でもよいし、情報を分担ごとの複数のセクションに分けて、それぞれを独立した情報として別々に署名を付与してもよい。しかし、後者の場合には情報間の関連性が失われないように配慮すること。				
	2. 共同作業における情報入力のワークフローが管理でき、そのワークフローに沿った制御が可能であること				
	3. ワークフローに沿ったログが記録されること				
	(6) システムの改造や保守等で診療録等に触れる場合の管理				
	1. 運用管理規程を整備し、定期的に監査すること。				
	2. アクセスログを定期的に監査すること。				
	(7) 機器・ソフトウェアの品質管理				
	1. システムを構成するソフトウェアの構成管理を行い、不正な変更が検知できること。				
	また検知された場合は、バックアップ等を用いて原状回復できること。				
	(8) 誤入力の防止				
	1. 過失は起こるものとの発想で、ヒヤリ・ハット事例等をもとに、誤入力防止のシステム的対策を施すこと。				
	2. 誤入力の発生状況を監察し、誤入力防止の対策が有効かどうか定期的に評価し、不十分な場合は、誤入力防止の仕組み及び方法を是正すること。(オーダ画面の薬剤配置、色分け、限度量・限度回数チェック、禁忌チェック、リストバンドによる本人チェック等)				
	(9) ルールの遵守				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	1. 運用管理規程に書かれたルールは確実に遂行されることが必要であり、確実を期すための内部監査を効果的に実施することは必須である				
	これを医療機関等の内部で適切かつ効果的に遂行することが期待できない場合は、第三者に委託することを考慮すべきである。				
	2. 組織内での運用プロセスが標準に準拠されたもの(ISO9000、ISMS 等)に沿って構築されていることを、必須ではないが強く推奨する。				
	7.2 見読性の確保について				
	(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。				
	(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。				
	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) 見読目的に応じた応答時間とスループット				
	1. 診療目的				
	① 外来診療部門においては、患者の前回の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。				
	② 入院診療部門においては、入院中の患者の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること				
	2. 患者への説明				
	① 患者への説明が生じた時点で速やかに検索表示もしくは書面に表示できること。なお、この場合の“速やかに”とは、数分以内である				
	3. 監査				
	① 監査当日に指定された患者の診療録等を監査に支障のない時間内に検索表示もしくは書面に表示できること				
	4. 訴訟等				
	① 所定の機関より指定された日までに、患者の診療録等を書面に表示できること。				
	② 保存場所が複数ある場合、各保存場所毎に見読手段を用意し、その操作方法を明示すること				
	(4) システム障害対策としての冗長性の確保				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	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手段を用意すること。				
	(5) システム障害対策としてのバックアップデータの保存				
	システムの永久ないし長時間障害対策として、日々バックアップデータを採取すること				
	(以下、推奨されるガイドライン)				
	(1) バップアップサーバ				
	システムが停止した場合でも、バップ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。				
	(2) 見読性を確保した外部保存機能				
	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) 遠隔地のデータバックアップを使用した検索機能				
	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。				
	7.3 保存性の確保について				
	(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。				
	(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。				
	保管及び取扱いに関する作業履歴を残すこと。				
	2. システムが情報を保存する場所(内部、可搬媒体)を明示し、その場所ごとの保存可能用量(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. サーバの設置場所には、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				
	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。				
	5. 各保存場所における情報が破損した時に、バックアップされたデータを用いて破損前の状態に戻せること				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	もし、破損前と同じ状態に戻せない場合は、失われた範囲が容易にわかること。				
	(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. 記録媒体の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				
	(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				
	1. システムの変更に際して、以前のシステムで蓄積した情報の継続的利用を図るための対策を実施すること。				
	システム導入時に、契約等でシステム導入業者にデータ移行に関する情報開示条件を明確にし、旧システムから新システムに移行する場合に、システム内のデータ構造が分からないことに起因するデータ移行の不能を防止すること				
	開示条件には倒産・解散・取扱い停止などの事態にも対応できることを含める必要がある。				
	2. 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. マスタDB 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。				
	(以下、推奨されるガイドライン)				
	(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. 電子的に保存された診療録等の情報にアクセスするシステムでは、ウイルス対策ソフト等を導入し、定期的にウイルスの検出を行い、ウイルスが発見された場合には直ちに駆除すること。				
	ウイルス定義ファイルは常に最新の状態に保つように、端末の運用管理を徹底すること。				
	2. アンチウイルスゲートウェイ等を導入し、院内のシステムにウイルスが侵入することを防止すること				
	ウイルス定義ファイル更新用のサーバを導入する等の方策により、各端末に導入したウイルス対策ソフトの定義ファイル及びバージョンが、常に最新の状態に保たれるようにシステム的な対策を施すこと				
	(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、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。				
	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. 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				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	改ざん等による情報の破壊が行われていないことが証明された場合は、元の情報が破壊された場合にその複製を診療に用い、保存義務を満たす情報として扱うこととする。				
	(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. 記録媒体に関しては、あるレベル以上の品質が保証された媒体に保存すること。				
	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は、RAID-1 もしくはRAID-5 相当のディスク障害に対する対策を取ること。				
	7.4 法令で定められた記名・押印を電子署名で行うことについて				
	(1) 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. 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、少なくとも同様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。				
	2. 「電子署名に係る地方公共団体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すべ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。				
	(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. タイプスタンプは、「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、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事。				
	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に留意しながら適切に対策を講じる必要がある。				
	(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。				
8 診療録及び診療諸記録を外部に保存する際の基準					
	8.1 電子媒体による外部保存をネットワークを通じて行う場合				
	8.1.1 電子保存の3 基準の遵守				
	(1) 電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保				
	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の受託先の機関と外部保存の委託元の医療機関等が、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。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	② 電気通信回線上で「改ざん」されていないことを保証すること 電気通信回線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				
	③ リモートログイン制限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、リモートログインが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				
	(2) 電気通信回線や外部保存を受託する機関の障害等による見読性の確保				
	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) 電気通信回線や外部保存を受託する機関の障害等に対する保存性の確保				
	① 外部保存を受託する機関において保存したことを確認すること 外部保存の受託先の機関におけるデータベースへの保存を確認した情報を受け取ったのち、委託元の医療機関等における処理を適切に行うこと。				
	② 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、外部保存の受託先の機関はその区別を行い、混同による障害を避けるとともに、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 電気通信回線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 電気通信回線や受託先の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おこなうこと。				
	④ 情報の破壊に対する保護機能や復旧の機能を備えること 故意または過失による情報の破壊がおこらないよう、情報保護機能を備えること				
	万一破壊がおこった場合に備えて、必要に応じて回復できる機能を備えること。				
	(以下、推奨されるガイドライン)				
	(1) 電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保				
	① 診療録等を転送する際にメッセージ認証機能を用いること 通信時の改ざんをより確実に防止するために、一連の業務手続内容を電子的に保証、証明することが望ましい。メッセージ認証機能によりメッセージ内容が確かに本人の送ったものであること、その真正性について公証能力、証憑能力を有するものであることを保証する。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	メッセージ認証機能の採用に当たっては保存する情報の同一性、真正性、正当性を厳密に証明するためにハッシュ関数や電子透かし技術等を用いることが望ましい。				
	(2) 電気通信回線や外部保存を受託する機関の障害等による見読性の確保				
	① 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、ネットワークや受託先の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が望ましい。				
	(3) 電気通信回線や外部保存を受託する機関の障害等に対する保存性の確保				
	① 標準的なデータ形式及び転送プロトコルを採用すること システムの更新等にともなう相互利用性を確保するために、データの移行が確実にできるように、標準的なデータ形式を用いることが望ましい。				
	② 電気通信回線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				
	受先の機関は、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が望ましい。				
	8.1.2 外部保存を受託する機関の限定				
	① 病院、診療所に保存する場合				
	外部保存を受託する機関は、病院や診療所の内部で診療録等を保存する必要があり、病院や診療所の敷地外に保存することはできない。				
	② 医療法人等が適切に管理する場所に保存する場合				
	当該場所については、医療法に基づき医療機関としての届け出がなされていたり、医師会立の病院に併置されている等の場合は、本項の①に位置づけてよい				
	個別の医療法人ないしは医療機関等が、危機管理上の目的等で外部保存を行おうとする場合は、保存主体である医療機関等の責任を明確化し安全管理措置を具体的に示した本項の④に従うこと				
	③ 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				
	ア) 法律や条例により、保存業務に従事する個人もしくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。				
	イ) 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、原則として保存主体の医療機関等のみがデータ内容を閲覧できることを技術的に担保できること。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	ウ) イ)を含め、適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及びCertified Information Systems Auditor (ISACA 認定)等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。				
	④ 医療機関等が震災対策等の危機管理上の目的で確保した安全な場所				
	(ア) 医療機関等が、保存に係る情報処理機器を自らの所有物として保持し、電気通信回線の確保や管理を保存主体である医療機関等の責任で行えるこ				
	診療録等の保存された情報に係る責任を自ら担保でき、電子保存のための医療機関等以外の場所を電源設備等を含めて自ら確保するか、または、適切な利用形態で借り受けて行う保存形態であること				
	(イ) 保存主体の医療機関等のみが保存情報にアクセス(保存情報の変更・修正・参照等)できることを診療録等の保存された情報の暗号化等の措置により技術的に担保できること				
	(ウ) 安全な場所を提供または管理する外部保存受託機関が適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及びCertified Information Systems Auditor(ISACA 認定)等の適切な能力を持つ監査人の外部監査を定期的に受ける等により確認されていること。				
	民間企業が外部保存受託機関である場合はプライバシーマーク制度等の公正な第三者の認定を受けていること。				
	(エ) 外部保存受託機関に対して、医療情報等の守秘に関連した事項及び保存性確保のための電源管理等の厳格なルールを委託契約書等で管理者や電子保存作業従事者等のペナルティを含めて設定していること				
	(以下、推奨されるガイドライン)				
	「②医療法人等が適切に管理する場所に保存する場合」の場合、保存を受託した機関全体としてのより一層の自助努力を患者・国民に示す手段として、個人情報保護もしくは情報セキュリティマネージメントの認定制度である、プライバシーマークやISMS 認定等の第三者による認定の取得等も推奨される。				
	、「③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」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、上記のような第三者による認定制度も検討されたい				
	8.1.3 個人情報の保護				
	(1) 診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護				
	① 秘匿性の確保のための適切な暗号化をおこなうこと 秘匿性確保のために電気通信回線上は適切な暗号化を行い転送すること				
	② 通信の起点・終点識別のための認証をおこなうこと 外部保存を委託する医療機関等と受託する機関間の起点・終点の正当性を識別するために相互に認証を行うこと。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	通信手段によって、起点･終点の識別方法は異なる。例えば、インターネットを用いる場合は起点・終点の識別はIP パケットを見るだけでは確実にはできない				
	起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の医療機関等と受託先の機関を確実に相互に認証しなければならない				
	用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。				
	(2) 診療録等の外部保存を受託する機関内での個人情報保護				
	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機関内の個人情報保護については「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」において考え方が示されている。				
	「Ⅲ 医療・介護関係事業者の義務等」の「4. 安全管理措置、従業者の監督及び委託先の監督（法第20 条～第22 条）」及び本指針6 章を参照し、適切な管理を行なうこと。				
	(3) 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。				
	患者は自分の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。				
	② 外部保存終了時の説明				
	外部保存された診療録等が、予定の期間を経過した後に廃棄等により外部保存の対象から除かれる場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分であるが、医療機関や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。				
	③ 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				
	④ 患者本人の同意を得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の同意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、理解を得る必要がある				
	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。				
	8.1.4 責任の明確化				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	(1) 電子保存の3 条件に対する責任				
	① 管理責任を明確にすること 媒体への記録や保存、伝送等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、外部保存を受託する機関や、これらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの製造業者に行わせてもよい。				
	② 説明責任を明確にすること 外部保存の目的や利用者を含めた保存システムの管理運用体制等について、患者や社会に対して十分に説明する責任については、委託元の医療機関等が主体になって対応する必要がある				
	この際、個人情報の保護について留意しつつ、運用体制に関する実際の説明については、外部保存を受託する機関や、これらの契約先の電気通信回線提供事業者、機器やソフトウェアの製造業者にさせてもよい				
	③ 結果責任を明確にすること 電気通信回線を通じて伝送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。				
	委託元と受託先の機関や電気通信回線提供事業者等の間の契約事項に関しては、受託先の機関や、これらの機関と契約した電気通信回線提供事業者等が、委託元の医療機関等に対して責任を負う必要があり、法令に違反した場合はその責任も負う				
	(2) 通信経路の各課程における責任の所在の明確化				
	診療録等の外部保存に関する委託元の医療機関等、受託先の機関及び電気通信回線提供者の間で、次の事項について管理･責任体制を明確に規定して、契約等を交わすこと。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	・委託元の医療機関等で発生した診療録等を、受託先の機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作 ・委託元の医療機関等が電気通信回線に接続できない場合の対処 ・受託先の機関が電気通信回線に接続できなかった場合の対処 ・電気通信回線の経路途中が不通または著しい遅延の場合の対処 ・受託先の機関が受け取った保存情報を正しく保存できなかった場合の対処 ・委託元の医療機関等が、受託先の機関内の保存情報を検索できなかった場合及び返送処理の指示が不成功であった場合の対処 ・委託元の医療機関等の操作とは無関係に、受託先の機関のシステムに何らかの異常があった場合の対処 ・受託先の機関内でやむを得ず個人情報にアクセスしなくてはならなくなった場合の委託元の医療機関等への承認を求める手続き事項、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委託元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 ・伝送情報の暗号化に不具合があった場合の対処 ・委託元の医療機関等と受託先の機関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 ・委託元の医療機関等による受託先の機関における外部保存の取扱いについて監督する方法 ・外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の処置 ・委託元の医療機関等または受託先の機関が、外部保存を中止する場合の対処 ・外部保存に関する契約終了後の診療録等の扱いの取り決め				
	8.1.5 留意事項				
	電気通信回線を通じて外部保存を行い、これを受託先の機関において可搬型媒体に保存する場合にあっては、「8.2 電子媒体による外部保存を可搬型媒体を用いて行う場合」に掲げる事項についても十分留意すること。				
	8.2 電子媒体による外部保存を可搬型媒体を用いて行う場合				
	8.2.1 電子保存の3 基準の遵守				
	(1) 搬送時や外部保存を受託する機関の障害等に対する真正性の確保				
	① 委託元の医療機関等、搬送業者及び受託機関における可搬型媒体の授受記録を行うこと。 可搬型媒体の授受及び保存状況を確実にし、事故、紛失や窃盗を防止することが必要である				
	他の保存文書等との区別を行うことにより、混同を防止しなければならない。				
	② 媒体を変更したり、更新したりする際に、明確な記録を行うこと				
	(2) 搬送時や外部保存を受託する機関の障害等に対する見読性の確保				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	① 診療に支障がないようにすること 患者の情報を可搬型媒体で外部に保存する場合、情報のアクセスに一定の搬送時間が必要であるが、患者の病態の急変や救急対応等に備え、緊急に診療録等の情報が必要になる場合も想定しておく必要がある。				
	② 監査等に差し支えないようにすること				
	監査等は概ね事前に予定がはっきりしており、緊急性を求められるものではないことから、搬送に著しく時間を要する遠方に外部保存しない限りは問題がないと考えられる。				
	(3) 搬送時や外部保存を受託する機関の障害等における保存性の確保				
	① 標準的なデータ形式の採用 システムの更新等にともなう相互利用性を確保するために、データの移行が確実にできるように、標準的なデータ形式を用いることが望ましい。				
	② 媒体の劣化対策 媒体の保存条件を考慮し、例えば、磁気テープの場合、定期的な読み書きを行う等の劣化対策が必要である。				
	③ 媒体及び機器の陳腐化対策 媒体や機器の陳腐化に対応して、新たな媒体または機器に移行することが望ましい。				
	8.2.2 個人情報の保護				
	(1) 診療録等の記録された可搬型媒体が搬送される際の個人情報保護				
	可搬型媒体の遺失や他の搬送物との混同について、注意する必要がある				
	(2) 診療録等の外部保存を受託する機関内における個人情報保護				
	① 外部保存を受託する機関における医療情報へのアクセスの禁止				
	診療録等の外部保存を受託する機関においては、診療録等の個人情報の保護を厳格に行う必要がある。受託先の機関の管理者であっても、受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である				
	② 障害発生時のアクセス通知				
	診療録等を保存している設備に障害が発生した場合等で、やむをえず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない				
	③ 外部保存を受託する機関との守秘義務に関する契約				
	診療録等の外部保存を受託する機関は、法令上の守秘義務を負っていることからも、委託元の医療機関等と受託先の機関、搬送業者との間での責任分担を明確化するとともに、守秘義務に関する事項等を契約に明記する必要がある。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	④ 外部保存を委託する医療機関等の責任				
	診療録等の個人情報の保護に関する責任は、最終的に、診療録等の保存義務のある委託元の医療機関等が責任を負わなければならない				
	委託元の医療機関等は、上記の受託先の機関における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。				
	（以下、推奨されるガイドライン）				
	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				
	② 外部保存終了時の説明				
	医療機関等や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。				
	③ 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				
	④ 患者本人の同意を得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の同意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、理解を得る必要がある				
	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。				
	8.2.3 責任の明確化				
	(1) 電子保存の3 条件に対する責任の明確化				
	① 管理責任 媒体への記録や保存等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託先の機関に行わせることは問題がない。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	② 説明責任 利用者を含めた保存システムの管理運用体制について、患者や社会に対して十分に説明する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託先の機関にさせることは問題がない。				
	③ 結果責任 可搬型媒体で搬送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。				
	委託元の医療機関等と受託先の機関または搬送業者の間の契約事項に関しては、受託先の機関や搬送業者等が、委託元の医療機関等に対して責任を負う必要があり、法令に違反した場合はその責任も負うことになる。				
	(2) 事故等が発生した場合における責任の所在				
	診療録等を外部保存に関する委託元の医療機関等、受託先の機関及び搬送業者の間で、次の事項について管理・責任体制を明確に規定して、契約等を交わすこと。				
	・ 委託元の医療機関等で発生した診療録等を、外部機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作 ・ 委託元の医療機関等と搬送(業)者で可搬型媒体を授受する場合の方法と管理方法 ・ 事故等で可搬型媒体の搬送に支障が生じた場合の対処方法 ・ 搬送中に秘密漏洩があった場合の対処方法 ・ 受託先の機関と搬送(業)者で可搬型媒体を授受する場合の方法と管理方法 ・ 受託先の機関で個人情報を用いた検索サービスを行う場合、作業記録と監査方法、取扱い従業者等の退職後も含めた秘密保持に関する規定、秘密漏洩に関して患者からの照会があった場合の責任関係 ・ 受託先の機関が、委託元の医療機関等の求めに応じて可搬型媒体を返送することができなくなった場合の対処方法 ・ 外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の対処方法				
	8.3 紙媒体のままで外部保存を行う場合				
	8.3.1 利用性の確保				
	(1) 診療録等の搬送時間 外部保存された診療録等を診療に用いる場合、搬送の遅れによって診療に支障が生じないようにする対策が必要である。				
	① 外部保存の場所 搬送に長時間を要する機関に外部保存を行わないこと。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	② 複製や要約の保存 継続して診療をおこなっている場合等で、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、外部に保存する場合でも、診療に支障が生じないようコピーや要約等を内部で利用可能にしておくこと。				
	(2) 保存方法及び環境				
	① 診療録等の他の保存文書等との混同防止 診療録等を必要な利用単位で選択できるよう、他の保存文書等と区別して保存し、管理しなければならない。				
	② 適切な保存環境の構築 診療録等の劣化、損傷、紛失、窃盗等を防止するために、適切な保存環境・条件を構築・維持しなくてはならない。				
	8.3.2 個人情報の保護				
	(1) 診療録等が搬送される際の個人情報保護				
	① 診療録等の封印と遺失防止				
	診療録等は、目視による情報の漏出を防ぐため、運搬用車両を施錠したり、搬送用ケースを封印すること				
	診療録等の授受の記録を取る等の処置を取ることによって、その危険性を軽減すること。				
	② 診療録等の搬送物との混同の防止				
	他の搬送物との混同が予測される場合には、他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、危険性を軽減すること。				
	③ 搬送業者との守秘義務に関する契約				
	診療録等を搬送する業者は、「個人情報保護法」が成立し、法令上の守秘義務を負うことからも、委託元の医療機関等と受託先の機関、搬送業者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上、明記すること。				
	(2) 診療録等の外部保存を受託する機関内における個人情報保護				
	① 外部保存を受託する機関内で、患者の個人情報を閲覧する可能性のある場合				
	診療録等の外部保存を受託し、検索サービス等を行う機関は、サービスの実施に最小限必要な情報の閲覧にとどめ、その他の情報は、閲覧してはならない				
	情報を閲覧する者は特定の担当者に限ることとし、その他の者が閲覧してはならない。				
	外部保存を受託する機関は、個人情報保護法による安全管理義務の面から、委託元の医療機関等と受託先の機関、搬送業者の間で、守秘義務に関する事項や、支障があった場合の責任体制等について、契約を結ぶ必要がある。				
	② 外部保存を受託する機関内で、患者の個人情報を閲覧する可能性のない場合				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	診療録等の外部保存を受託する機関は、もっぱら搬送ケースや保管ケースの管理のみを実施すべきであり、診療録等の内容を確認したり、患者の個人情報を閲覧してはならない。				
	これらの事項について、委託元の医療機関等と受託先の機関、搬送業者の間で契約を結ぶ必要がある。				
	③ 外部保存を委託する医療機関等の責任				
	委託元の医療機関等は、上記の受託先の機関における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。				
	（以下、推奨されるガイドライン）				
	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。患者は自分の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。				
	② 外部保存終了時の説明				
	外部保存された診療録等が、予定の期間を経過した後に廃棄等により外部保存の対象から除かれる場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分であるが、医療機関等や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。				
	③ 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				
	④ 患者本人の同意を得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の同意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、理解を得る必要がある				
	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。				
	8.3.3 責任の明確化				
	(1) 責任の明確化				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	① 管理責任 診療録等の外部保存の運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託先の機関に行わせることは問題がない。				
	② 説明責任 利用者を含めた管理運用体制について、患者や社会に対して十分に説明する責任については委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託先の機関にさせることは問題がない。				
	③ 結果責任 診療録等を搬送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。				
	委託元の医療機関等と受託先の機関や搬送業者等の間の契約事項に関して、受託先の機関や搬送業者等が、委託元の医療機関等に対して責任を負う必要があり、法令に違反した場合はその責任も負うことになる。				
	(2) 事故等が発生した場合における責任の所在				
	診療録等を外部保存に関する委託元の医療機関等、受託先の機関及び搬送業者の間で、次の事項について管理・責任体制を明確に規定して、契約等を交わすこと。				
	・ 委託元の医療機関等で発生した診療録等を、外部機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作 ・ 委託元の医療機関等と搬送(業)者で診療録等を授受する場合の方法と管理方法 ・ 事故等で診療録等の搬送に支障が生じた場合の対処方法 ・ 搬送中に秘密漏洩があった場合の対処方法 ・ 受託先の機関と搬送(業)者で診療録等を授受する場合の方法と管理方法。 ・ 受託先の機関で個人情報を用いた検索サービスを行う場合、作業記録と監査方法 ・ 取扱い従業者等の退職後も含めた秘密保持に関する規定、秘密漏洩に関して患者から照会があった場合の責任関係 ・ 受託先の機関が、委託元の医療機関等の求めに応じて診療録等を返送することができなくなった場合の対処方法 ・ 外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の対処方法				
	8.4 外部保存全般の留意事項について				
	8.4.1 運用管理規程				
	外部保存に係る運用管理規程を定めることが求められており、考え方及び具体的なガイドラインは、「6.3 組織的安全管理対策」の項を参照のこと				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	8.4.2 外部保存契約終了時の処理について				
	診療録等が高度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、委託側の医療機関等及び受託側の機関双方で一定の配慮をしなくてはならない。注意すべき点は、診療録等を外部に保存していること自体が院内掲示等を通じて説明され、患者の同意のもとに行われていることである。				
	診療録等の外部保存を委託する医療機関等は、受託先の機関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				
	受託先の機関も、委託先の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、処理を行った旨を委託先の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側と受託側で取り交わす契約書にも明記をしておく必要がある				
	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ものを作成しておくべきである。				
	委託先、受託先双方に厳正な取扱いを求めるのは、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、そのことに十分なことに留意しなければならない。				
	〈紙媒体、可搬媒体で保存する場合の留意点〉				
	紙媒体や可搬型媒体での外部保存する場合は、原則として上記の点に注意すれば大きな問題はない。ただし、患者の個人情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索記録も機密保持できる状態で廃棄しなければならない。				
	委託先、受託先が負う責任は、先に述べた通りであり、紙媒体、可搬媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことには十分留意する必要がある。				
	〈電気通信回線を通じて外部保存する場合〉				
	電気通信回線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				
	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。				
	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委託側、受託側が確実に確認できるようにしておかなくてはならない。				
	8.4.3 保存義務のない診療録等の外部保存について				
	情報管理体制確保の観点から、バックアップ情報等も含め、記録等を破棄せず保存している限りは本章ガイドラインの取扱いに準じた形で保存がなされること。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	個人情報保護関連各法の趣旨を十分理解した上で、各種指針及び本ガイドライン6 章の安全管理等を参照して管理に万全を期す必要がある。				
9 診療録等をスキャナ等により電子化して保存する場合について					
	9.1 共通の要件				
	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること				
	スキャン等を行なう前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在したりすることで、スキャンによる電子化で情報が欠落することがないことを確認すること。				
	・ 診療情報提供書等の紙媒体の場合、300dpi、RGB 各色8 ビット（24 ビット）以上でスキャンを行なうこと。 ・ 放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン1.1 版（平成14 年6 月）」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予定である。 ・ このほか心電図等の波形情報やポラロイド撮影した情報等、さまざまな対象が考えられる。一般的に極めて精細な精度が必要なもの以外は300dpi、24 ビットのカラースキャンで十分と考えられるが、あくまでも医療に関する業務等に差し支えない精度が必要であり、その点に十分配慮すること。 ・ 一般の書類をスキャンした画像情報はTIFF形式またはPDF形式で保存することが望ましい。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮をおこなう場合は医療に関する業務等に支障がない精度であること、及びスキャンの対象となった紙等の破損や汚れ等の状況も判定可能な範囲であることを念頭におこなう必要がある。放射線フィルム等の医用画像をスキャンした情報はDICOM 等の適切な形式で保存すること。				
	2. 改ざんを防止するため、医療機関等の管理責任者は以下の措置を講じること				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	・スキャナによる読み取りに係る運用管理規程を定めること ・スキャナにより読み取った電子情報ともとの文書等から得られる情報との同一性を担保する情報作成管理者を配置すること ・スキャナで読み取った際は、作業責任者(実施者または管理者)が電子署名法に適合した電子署名等を遅滞なく行い、責任を明確にすること。 なお、電子署名法に適合した電子署名とは、これを行うための私有鍵の発行や運用方法を適正に管理することにより、本人だけが行うことができる電子署名を指す。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い場合は、少なくとも同様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。 ・スキャナで読み取る際は、読み取った後、遅滞なくタイムスタンプを電子署名を含めたスキャン文書全体に付与すること。				
	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、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、スキャン後の電子化文書を利用する第三者がタイムスタンプを検証することが可能である事。				
	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。				
	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に留意しながら適切に対策を講じる必要がある。				
	3. 情報作成管理者は、上記運用管理規程に基づき、スキ正な手続で確実に実施される措置を講じること。				
	4. 緊急に閲覧が必要になったときに迅速に対応できるよう、停電時の補助電源の確保、システムトラブルに備えたミラーサーバーの確保等の必要な体制を構築すること				
	5. 個人情報の保護のため個人情報保護法を踏まえた所要の取扱いを講じること。				
	特に電子化後のもとの紙媒体やフィルムを破棄する場合、シュレッダー等で個人識別不可能な状態にしたうえで破棄しなければならない(医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン、及び本指針第6 章参照)。				
	9.2 診療等の都度スキャナ等で電子化して保存する場合				
	9.1 の対策に加えて、改ざんを防止するため情報が作成されてから、または情報を入手してから一定期間以内にスキャンを行うこと。				
	・一定期間とは改ざんの機会が生じない程度の期間で、通常は遅滞なくスキャンを行なわなければならない				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	時間外診療等で機器の使用ができない等の止むを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行うこととする				
	9.3 過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合				
	9.1 の対策に加えて、以下の対策を実施すること。				
	1. 電子化をおこなうにあたって事前に対象となる患者等に、スキャナ等で電子化をおこなうことを掲示等で周知し、異議の申し立てがあった場合はスキャナ等で電子化をおこなわないこと。				
	2. かならず実施前に実施計画書を作成すること。実施計画書には以下の項目を含むこと。				
	・運用管理規程の作成と妥当性の評価。評価は大規模医療機関等にあっては外部の有識者を含む、公正性を確保した委員会等でおこなうこと(倫理委員会を用いることも可)。 ・作業責任者の特定。 ・患者等への周知の手段と異議の申し立てに対する対応。 ・相互監視を含む実施の体制。 ・実施記録の作成と記録項目。(次項の監査に耐えうる記録を作成すること。) ・事後の監査人の選定と監査項目。 ・スキャン等で電子化をおこなってから紙やフィルムを破棄するまでの期間、及び破棄の方法。				
	3. 医療機関等の保有するスキャナ等で電子化をおこなう場合の監査をシステム監査技術者やCertified Information Systems Auditor(ISACA 認定)等の適切な能力を持つ外部監査人によっておこなうこと。				
	4. 外部事業者に委託する場合は、9.1 の要件を満たすことができる適切な事業者を選定する				
	適切な事業者とみなすためには、少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認する必要がある				
	実施に際してはシステム監査技術者やCertified Information Systems Auditor(ISACA 認定)等の適切な能力を持つ外部監査人の監査を受けることを含めて、契約上に十分な安全管理をおこなうことを具体的に明記すること。				
	9.4(補足) 運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合				
	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	・診療情報提供書等の紙媒体の場合、原則として300dpi、RGB 各色8 ビット（24 ビット）以上でスキャンすること。これは紙媒体が別途保存されるものの、電子化情報に比べてアクセスの容易さは低下することは避けられず、場合によっては外部に保存されるかも知れない。したがって運用の利便性のためとは言え、電子化情報はもとの文書等の見読性を可能な限り保つことが求められるからである。ただし、もともとプリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度をさげることもできる。				
	・放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン1.1 版（平成14 年6 月）」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予定である。				
	・このほか心電図等の波形情報やポラロイド撮影した情報等、さまざまな対象が考えられる。一般的に極めて精細な精度が必要なもの以外は300dpi、24 ビットのカラースキャンで十分と考えられるが、あくまでも医療に関する業務等に差し支えない精度が必要であり、その点に十分配慮すること。				
	・一般の書類をスキャンした画像情報はTIFF形式またはPDF形式で保存することが望ましい。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮をおこなう場合は医療に関する業務等に支障がない精度であること、及びスキャンの対象となった紙等の破損や汚れ等の状況も判定可能な範囲であることを念頭におこなう必要がある。放射線フィルム等の医用画像情報をスキャンした情報はDICOM 等の適切な形式で保存すること。				
	2. 管理者は、運用管理規程を定めて、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。				
	3. 緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。				
	4. 個人情報の保護のため個人情報保護関連各法を踏まえた所要の取扱いを講じること。				
	特に電子化後のもとの紙媒体やフィルムの安全管理もおろそかにならないように注意しなければならない。				
	10 運用管理について				
	以下の項目を運用管理規程に含めること。				
	(1) 一般管理事項				
	① 総則 a) 理念 b) 対象情報				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	② 管理体制 a) システム管理者、運用責任者の任命 b) 作業担当者の限定 c) マニュアル・契約書等の文書の管理 d) 監査体制と監査責任者の任命 e) 苦情の受け付け窓口の設置 f) 事故対策 g) 利用者への周知法				
	③ 管理者及び利用者の責務 a) システム管理者や運用責任者の責務 b) 監査責任者の責務 c) 利用者の責務				
	④ 一般管理における運用管理事項 a) 来訪者の記録・識別、入退の制限等の入退管理 b) 情報システムへのアクセス制限、記録、点検等のアクセス管理 c) 委託契約における安全管理に関する条項 d) 個人情報の記録媒体の管理（保管・授受等） e) 個人情報を含む媒体の廃棄の規程 f) リスクに対する予防、発生時の対応				
	⑤ 教育と訓練 a) マニュアルの整備 b) 定期または不定期なシステムの取扱い及びプライバシー保護に関する研修 c) 従業者に対する人的安全管理措置 ・ 医療従事者以外との守秘契約 ・ 従事者退職後の個人情報保護規程				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	⑥ 業務委託の安全管理措置 a) 業務委託契約における守秘条項 b) 再委託の場合の安全管理措置事項 c) システム改造及び保守でのデータ参照 ・ 保守要員専用のアカウントの作成及び運用管理 ・ 作業時の病院関係者の監督 ・ 保守契約における個人情報保護の徹底 ・ メッセージログの採取と確認				
	⑦ 監査 a) 監査の内容 b) 監査責任者の任務				
	(2) 電子保存の為の運用管理事項				
	① 真正性確保 a) 作成者の識別及び認証 b) 情報の確定手順と、作成責任者の識別情報の記録 c) 更新履歴の保存 d) 代行操作の承認記録 e) 一つの診療録等を複数の医療従事者が共同して作成する場合の管理 f) 機器・ソフトウェアの品質管理				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	② 見読性確保 a) 情報の所在管理 b) 見読化手段の管理 c) 見読目的に応じた応答時間とスループット ・ 診療目的 ・ 患者説明 ・ 監査 ・ 訴訟 d) システム障害対策 ・ 冗長性 ・ バックアップ ・ 緊急対応				
	③ 保存性確保 a) ソフトウェア・機器・媒体の管理（例えば、設置場所、施錠管理、定期点検、ウイルスチェック等） 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策 b) 不適切な保管・取扱いによる情報の滅失、破壊の防止策 c) 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策 d) 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策 e) 万が一に備えての考慮対策 f) 情報の継続性の確保策（例えば、媒体の劣化対策等） g) 情報保護機能策（例えば、バックアップ等）				
	④ 相互利用性確保 a) システムの改修に当たっての、データ互換性の確保策 b) システムの更新に当たっての、データ互換性の確保策				
	⑤ スキャナ読み取り書類の運用 a) スキャナ読み取り電子情報と元の文書等との同一性を担保する情報作成管理者の任命 スキャナ読み取り電子情報への作業責任者(実施者または管理者)の電子署名法に適合した電子署名 b) スキャナ読み取り電子情報への正確性な読みとり時刻の付加				
	(3) ネットワークによる外部保存に当たっての「医療機関等としての管理事項」				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	可搬型媒体による外部保存、紙媒体による外部保存に当たっては、本項を参照して「医療機関等としての管理事項」を作成すること。				
	① 管理体制と責任 a) 委託に値する事業者と判断した根拠の記載 受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。 b) 委託元での管理責任者 c) 受託機関への監査体制 d) 保存業務受託機関との責任分界点 e) 受託機関の管理責任、説明責任、結果責任の範囲を明文化した契約書等の文書作成と保管 f) 事故等が発生した場合における対処責任、障害部位を切り分ける責任所在を明文化した契約書等の文書作成と保管 受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。				
	② 外部保存契約終了時の処理 受託先に診療録等が残ることがない様な処理法 a) 受託先に診療録等が残ることがないことの受託先との契約、管理者による確認				
	③ 真正性確保 a) 相互認証機能の採用 b) 電気通信回線上で「改ざん」されていないことの保証機能 c) リモートログイン制限機能				
	④ 見読性確保 a) 緊急に必要になることが予測される医療情報の見読性の確保手段 b) 緊急に必要になるとまではいえない医療情報の見読性の確保手段 ＊ 上記事項は推奨				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	⑤ 保存性確保 a) 外部保存を受託する機関での保存確認機能 b) 標準的なデータ形式及び転送プロトコルの採用 ＊ 上記事項は推奨 c) 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確保 d) 電気通信回線や外部保存を受託する機関の設備の劣化対策 e) 電気通信回線や外部保存を受託する機関の設備の互換性確保 ＊ 上記事項は推奨 f) 情報保護機能				
	⑥ 診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護 a) 秘匿性の確保のための適切な暗号化 b) 通信の起点・終点識別のための認証				
	⑦ 診療録等の外部保存を受託する機関内での個人情報の保護 a) 外部保存を受託する機関における個人情報保護 b) 外部保存を受託する機関における診療録等へのアクセス禁止 受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。 c) 障害対策時のアクセス通知 d) アクセスログの完全性とアクセス禁止				
	⑧ 患者への説明と同意 a) 診療開始前の同意 b) 患者本人の同意を得ることが困難であるが、診療上の緊急性がある場合 c) 患者本人の同意を得ることが困難であるが、診療上の緊急性が特にない場合				
	⑨ 受託機関への監査項目 a) 保存記録（内容、期間等） b) 受託機関側での管理策とその実施状況監査				