(4)	スキャナ読み取り書類の運用	スキャナ読取の対象にする文書の規程	A		・対象文書を定める	・システム管理者は、適宜、業務において規程通りの運用がなされていることを確認すること。
		スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	A	・適切な解像度のスキャナの使用	・スキャナ読み取りの運用管理を規程する	
		スキャナ読み取り電子情報への作業責任者の電子署名及び認証業務に関する法律に適合した電子署名・タイムスタンプ	A	・電子署名・タイムスタンプ環境の構築		
		診療の都度、スキャンするタイミングの規程	A	・タイムスタンプ機能	・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(1～2日程度以内)にスキャンを行うことを運用管理規程で定め、遅滞なくスキャンを行うこと	

付表3　外部保存における運用管理の例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理基準項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①、⑨	管理体制と責任	管理体制の構築、受託する機関の選定、責任範囲の明確化、契約	B		管理体制の構築、受託する機関の評価・選定、契約	この規程は、○○病院(以下「当院」という)において、診療録及び診療諸記録(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管するの仕組みと管理に関する事項を定めたものである。本規程の付表に、当院における管理体制(運用責任者、システム管理者、各作業実務者(外部の業業務委託者を含む))、XXへの監査体制(監査者)、を定める。 なお、システム管理者は、保管を委託するXXは「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する機関の選定基準」を満たしていることを適宜確認すること。XXが民間事業者等のデータセンター等の情報処理関連事業者である場合には、経済産業省が定めた「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」や業務形態によっては総務省が定めた「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」の要求事項を満たしていることを確認すること。
			C		管理体制の構築、受託する機関の評価・選定、契約	この規程は、○○病院(以下「当院」という)において、診療録及び診療諸記録(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管するための仕組みと管理に関する事項を定めたものである。運用責任者は院長とし、運用内容の管理実務および監査はΔΔに委託する。また、保管を受託するXXの評価、管理・監査を受託するΔΔへの評価を添付する。 なお、院長は、保管を委託するXXは「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する機関の選定基準」を満たしていることをΔΔに適宜確認すること。また、XXが民間事業者等のデータセンター等の情報処理関連事業者である場合には、経済産業省が定めた「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」や業務形態によっては総務省が定めた「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」の要求事項を満たしていることをΔΔに適宜確認すること。
		受託する機関への監査	A		受託する機関に対する保管記録の監査規程作成、契約	システム管理者は、XXにおける「診療記録」の保管内容を示す記録を監査し、正しいことを確認する。異常の発見時には直ちに運用責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。また、これらの確認記録を残す。
					受託する機関での管理策の承認、実施監査規程作成、契約	システム管理者は、XXにおける受託「診療記録」の管理策を精査し、承認する。その管理策の実施状況を必要時に監査する。異常の発見時には直ちに運用責任者に報告すると共に、XXに対し対処を指示し、結果を確認する。また、これらの監査記録を残す。
		責任の明確化	A		通常運用における責任、事故責任の分界点を定める	運用責任者は、定められた責任体制が維持されていることを確認する。
		動作の監査	B	委託する機関での送信記録、受託する機関での受信記録の保持	委託する機関での送信記録、受託する機関での受信記録の合致監査	システム管理者は、XXから「診療記録」の受信記録を受け取り、送信した「診療記録」との合致を確認する。また、確認した旨の作業記録を残す。異常の発見時には直ちに運用責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。
			C	(監査目的に耐える記録レベル、保存期間であること)	監査(上記を含む全)を第三者へ委託した場合は、定期的報告(6ヶ月程度)を受けること	運用責任者は、監査を委託したΔΔから、『XXからの「診療記録」の受信記録、送信した「診療記録」との合致を確認した』旨の報告を受け、確認後に報告内容の保管を行う。また、異常発生時には直ちに報告を受け、ΔΔと共に対処に着手する。
		不都合な事態への対処	A		受託する機関との間で、不都合な事態(異常の可能性も含む)の責任対処作業範囲を定める	運用責任者は「診療記録」流出の危険があると判断した時には、直ちに外部保存の運用を停止する。
②	外部保存契約終了時の処理		A		保管データの破棄契約と管理者による確認、守秘義務契約	【契約事項として】当院とXXとの契約終了時には、それまでに保管を受託した全ての「診療記録」を当院に戻す(あるいは、利用不可能な形で廃棄する)ことと、その結果につき当院の監査を受けるものとする。また、XXが受託期間中に異常への対応等で「診療記録」の内容にアクセスした場合、その内容についての守秘義務は、本保管委託契約終了後も有効である。
③	真正性確保	相互認証機能の採用	A	SSL/TLSあるいは相互認証付きVPNの使用	認証局を使う場合は、両機関でお互いに相手方の証明書を認証可能な認証局を選定すること。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方のなりすましが無いことを確認する。
		通信上で「改ざんされていない」ことの保証	A	SSL/TLSあるいはメッセージ認証付きのVPNの使用	認証局を使う場合は、両機関でお互いに相手方の証明書を認証可能な認証局を選定すること。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の確認において、通信上の改ざんの発見に努める。

④	見読性確保	情報の所在管理 見読化手段の管理 見読目的に応じた応答時間とスループット システム障害対策	A		付表2の見読性確保と同じ技術的対策・運用的対策がとられていることの確認	システム管理者は、XXにおける見読性対策が適切であることを確認する。監査者は必要に応じてXXの設備を監査する。
⑤	保存性確保	外部保存を受託する機関での保存確認機能	A	受託する機関との間で、改ざんされることの無いデータとして保存されたことを確認できる機能 、たとえばネットワークを介したStrageへの保管確認機能、あるいは 保存を委託する機関への保管内容送信機能(1時間～1日単位)	・付表2の保存性確保と同じ技術的対策・運用的対策がとられていることの確認 ・受託先での保存が確認された時点まで委託元でのデータ削除を行わない作業規程	システム管理者は、XXにおける保存性対策が適切であることを確認する。監査者は必要に応じてXXの設備を監査する。
		標準的なデータ形式及び転送プロトコルの採用	A	DICOM、HL7、標準コードの使用あるいはこれらへの変換機能		
		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	A		継続性の保証契約を交わす	【契約事項として】当院とXXは互いに各自のシステム変更に当たっては、相互にデータ通信の継続性に配慮し、変更内容が外部保存の障害にならないように協議をする。
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保護策	秘匿性の確保のための適切な暗号化	A	メッセージの暗号化が可能な通信手段 暗号の強度は、電子署名法に準じること		
		通信の起点・終点識別のための認証	A	SSL/TLSあるいは相互認証付きVPNの使用 暗号の強度は、電子署名法に準じること	認証局を使う場合は、両機関でお互いに相手方の証明書を認証可能な認証局を選定すること 双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方が正当であることを確認する。
⑦	外部保存を受託する機関内での個人情報保護策	外部保存を受託する機関における個人情報保護	A		受託する機関と受託する機関側における業務従事者への教育、守秘義務	監査者は必要に応じてXXを監査する。【契約事項として】①XXは当院から受けた保管委託を再委託してはならない ②XXは「診療記録」の保管業務に従事する従業員に対して「個人情報保護の重要性」の教育を年1回行う。また、その業務を離れた後も有効な守秘契約を当該従業員と交わすこと。
		外部保存を受託する機関における診療情報へのアクセス禁止	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログの監査	監査者は、XXにおける保管された「診療記録」及びアクセスログへのアクセス記録を監査する。
		外部保存を受託する機関における障害対策時のアクセス通知	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	アクセス許可、秘密保持に関する契約と受託する機関によるアクセスログの監査	【契約事項として】XXにおいては正当な理由無く、保管した「診療記録」及びアクセスログにアクセスしてはならない。出来る限り事前に当院の許可を得ることとし、やむを得ない事情で許可を得ずアクセスした場合は速やかに当院に報告するものとする。また、目的外に利用してはならないし、正当で明確な目的が無く他の媒体等に保管してはならない。
		外部保存を受託する機関におけるアクセスログの完全性とアクセス禁止	A	アクセスログファイルへのアクセス制御とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログへのアクセスの監査	
⑧	患者への説明	外部保存を行っている旨を院内掲示等を通じて周知すること	A		外部保存を行っている旨を院内掲示等を通じて周知すること	運用責任者は、外部保存していることの患者への周知(例、掲示内容)が計られていることを適宜確認する。
						付録 1. 管理体制・受託する機関との責任分担規程 2. XXに保管を委託する「診療記録」の定義 3. XXへの監査事項 4. XXとの契約

付録　（参考）外部機関と診療情報等を連携する場合に取り決めるべき内容

外部の機関と診療情報共有の連携等を行う場合に、連携する機関の間で取り決めるべき内容の参考として以下に記載する。

1. 組織的規約
   理念、目的
   管理と運営者の一覧、各役割と責任
   医療機関と情報処理事業者・通信事業者等との責任分界点
   免責事項、知的財産権に関する規程
   メンバの規約（メンバ資格タイプ、メンバの状況を管理する規約）、資金問題　等
2. 運用規則
   管理組織構成、日常的運営レベルでの管理方法
   システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知等）、データ維持、保存、バックアップ 、不具合の回復　等
3. プライバシ管理
   患者共通ID（もし、あるならば）の管理方法
   文書のアクセスと利用の一般則
   役割とアクセス権限のある文書種別の対応規約
   患者同意のルール
   非常時のガイド(ブレークグラス、システム停止時、等の条件)　等
4. システム構造
   全体構造、システム機能を構成する要素、制約事項
   連携組織外部との接続性（連携外部の組織とデータ交換方法）　等
5. 技術的セキュリティ
   リスク分析
   認証、役割管理、役割識別(パスワード規約、2要素認証等の識別方法)
   可搬媒体のセキュリティ要件　等
6. 構成管理
   ハードウェアやソフトウェアの機能更新、構成変更等の管理方法、新機能要素の追加承認方法　等

7. 監査
   何時、誰が監査し、適切な行動が取られるか

8. 規約の更新周期