付表3　外部保管における運用管理の例

管理事項番号	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、委託施設の選定、責任範囲の明確化、契約	B		管理体制の構築、委託施設の評価・選定、契約	この規程は、○○病院(以下「当院」という)において、法令に保存義務が規定されている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において保管する為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（管理責任者、運用管理者、各作業実務者(外部の実業務委託者を含む)）、XXへの監査体制(監査者)、を定める。また、保管を委託するXXへの評価を添付する。
			C		管理体制の構築、委託施設の評価・選定、契約	この規程は、○○病院(以下「当院」という)において、法令に保存義務が規定されている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において保管する為の仕組みと管理に関する事項を定めたものである。管理責任者は院長とし、運用内容の管理実務および監査は△△に委託する。また、保管を委託するXXの評価、管理・監査を委託する△△への評価を添付する。
		受託施設への監査	A		受託先に対する保管記録の監査規程作成、契約	運用管理者は、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管理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。
					受託先での管理策の承認、実施監査規程作成、契約	運用管理者は、XXにおける受信「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管理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		管理責任・説明責任・結果責任の分担を定める。	付表に各管理事項（7．1．4参照）の責任分界点を定める。
		動作の監査	B	委託元での送信記録、受託先での受信記録の保持 （監査目的に耐える記録レベル、保存期間であること）	委託元での送信記録、受託先での受信記録の合致監査	運用管理者は、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管理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（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	管理責任者は、監督を委託した△△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、△△と共に対処に着手する。
		異常時の対処	A		受託先との間で、異常時(異常の可能性も含む)の責任対処作業範囲を定める	管理責任者は「診療記録」流出の危険があると判断した時には、直ちに外部保管の運用を停止する。
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）こととし、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	委託元の医療機関への成りすまし防止	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、両施設間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事。	運用管理者は、記録による動作の監査において、委託元、受託先双方の成りすましが無い事を確認する。
		受託先施設への成りすまし防止	A		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。	
		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、両施設間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事。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。	運用管理者は、記録による動作の確認において、通信上の改竄の発見に努める。
		リモートログインの制限	A	ログインの記録 （正常なログインと不正なログインが識別可能な記録レベル、監査機関より長い保存期間であること）	ログイン記録の監査	運用管理者は、記録による動作の確認において、不正と疑われるログインが無い事を確認する。
④	見読性確保	緊急に必要になることが予測される診療情報の見読性の確保	A	院内システムにおいて、緊急に必要になることが予測される診療情報を格納するに充分な記憶容量	原本と同等の内容を院内に保持	運用管理者は、緊急時における「診療記録」のアクセスに支障が無いように、院内システムにおける記憶容量の過不足を管理する。
		緊急に必要になるとまではいえない診療情報の見読性の確保	A	可搬型媒体やバックアップ媒体からもデータが読み取れる手段があることが望ましい	外部保存委託したデータの、可搬型媒体へのコピーやバックアップを取り、 受託先施設とは異なる場所に保持しておく事が望ましい。委託元でも良い。	運用管理者は、ＸＸに委託した「診療記録」の、ＸＸ以外の場所にあるコピーやバックアップの存在について確認をし、アクセスが可能である事の確認をおこなう。
		ネットワークや受託先施設の障害等の場合による見読性の確保	A			
⑤	保存性確保	外部保存を受託する施設での保存確認機能	A	受託先施設との間で、改ざんされることの無いデータとして保存された事を確認できる機能　①ネットワークを介したStrage Commitment的機能　②保存記録の委託元への送信機能（1時間～1日単位）	左記推奨案が不可のときは、同等の事を運用で行う作業規定、あるいは、保存されているべきデータへの読み出しで確認する	運用管理者は、記録による動作の確認において、XXにおける保存が正常である事を確認する。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、変更内容が外部保管の障害にならないように協議をする。
		電気通信回線や外部保存を受託する施設の設備の劣化対策	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてＸＸの設備を監査する。【契約事項として】XXは保管設備の劣化に意を払い、機能の保全に努めなければならない。
		電気通信回線や外部保存を受託する施設の設備の互換性確保	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてＸＸの設備を監査する。【契約事項として】ＸＸは、保管データの全てがネットワーク経由で当院から読み出せる様に、保管設備のデータ互換性を維持しなければならない。
		情報保護機能	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてＸＸの設備を監査する。【契約事項として】ＸＸは、ＸＸの責に帰す保管データの故意または過失による破壊に備えて、回復できる機能を備えなければならない。
⑥	外部保存を受託する施設内での 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、両施設間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事 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。	運用管理者は、記録による動作の監査において、委託元、受託先双方が正当である事を確認する。
⑦	個人情報保護策	外部保存を受託する施設における個人情報保護	A		受託施設と「受託施設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施設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	委託元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施設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委託元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遅滞無く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などに保管してはならない。
		外部保存を受託する施設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	委託元によるアクセスログへのアクセスの監査	
⑧	患者への説明と同意	外部保存を行っている旨を院内掲示等を通じて周知し、同意を得ること	A		外部保存を行っている旨を院内掲示等を通じて周知し、同意を得ること	管理責任者は、外部保管している事の患者への周知が計られている事（例、掲示内容、位置）、また同意を得られなかった患者の「診療記録」の管理状況を適宜(例、1回/月)確認する。
						付録 1．管理体制･委託施設との責任分担規定 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

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