３省３ガイドラインで求められる事項の対応関係

※厚労省、総務省、経産省の医療関連３ガイドライン。それぞれのガイドラインの対応関係をまとめたものです。これをまとめないと、３ガイドラインすべてを遵守するのが難しいと思ったため。
※なお、ざっと作ったために誤りのある可能性があります。必ず原典をご確認ください。

			中項目・小項目は本文の項目そのままではなく、本文からアレンジしている場合がある		項目は短文化等のため水町にて変更している場合がある			行の統廃合をした方が、わかりやすい可能性もあり、要改善であることは理解している			A:最低限又は必要、B:推奨、C：その他	←表現ぶりの評価にもなるので、ABC曖昧な部分も残る。	
「厚生労働省「医療情報システムの安全管理に関するガイドライン」第5版	経済産業省「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」	総務省「クラウドサービス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第1版」	大項目	中No	中項目	小No	小項目	措置	ジャンル1	ジャンル2	ランク	該当ページ	水町コメント
2			本指針					対象は、医療に関する患者情報（個人識別情報）を含む情報及びその情報を扱うシステム	総論		C	13p	
仕様・運用方法等の文書化、監査・報告、責任者													
	4.1		情報処理事業者の管理者における情報保護責任					取り扱う個々の情報の価値、リスク、責任について受託元の医療機関等と考えを共通した上で、システム仕様、運用計画、事業継続計画等に合意する	総論		B	30p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	①	説明責任	システムの仕様や運用方法を明確に文書化	総論		A	22p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	①	説明責任	仕様や運用方法が当初の方針のとおりに機能しているかどうかを定期的に監査	監査等		A	22p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	①	説明責任	・監査結果をあいまいさのない形で文書化 ・監査の結果問題があった場合は、真摯に対応 ・対応の記録を文書化し、第三者が検証可能な状況にする	監査等		A	22p	

	4.1		情報処理事業者の管理者における情報保護責任	4.2	通常運用における責任	(1)	説明責任	システム文書として、ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと、定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告について提出可能な状態におくこと等を委託契約事項に含め、履行する	総論	監査等	A	経産30p-	
		2.3	クラウドサービス事業者の責任	2.3.1	通常運用における責任	(1)	説明責任	・提供するクラウドサービスの仕様、運用及びセキュリティ対策に関する事項の文書化 ・提供するクラウドサービスの仕様及び品質に関する説明及び必要な情報提供 ・提供するクラウドサービスに関する監査等の情報の提供	総論	監査等	A	総務26 p	
4.2.1			委託	(1)	通常運用における責任	③	PDCA	運用管理状況に対する定期的な監査、問題点の洗い出し、改善の責任分担、技術進展に配慮した定期的な再評価・再検討、その結果に基づき対策を行う際の医療機関等との協議について、契約事項に含める	委託	監督	B	24p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	②	管理責任	少なくとも管理状況の報告を定期的に受ける	監査等		A	22p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	②	管理責任	管理に関する最終的な責任の所在を明確にする等の監督を行う	監督		A	22p	意味が分かりづらい。医療機関等と請負事業者それぞれ責任者を定めるといったことかどうかが不明。それ
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	②	管理責任	個人情報保護の責任者を定める	組織的	監督	A	23p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	②	管理責任	電子化された個人情報の保護について一定の知識を有する責任者を決める	組織的	監督	A	23p	
		2.3	クラウドサービス事業者の責任	2.3.1	通常運用における責任	(2)	管理責任	・医療機関等の管理者に対するクラウドサービス事業者側の最終的な管理責任者の明確化 ・個人情報保護責任者を含むクラウドサービスの提供体制の明確化 ・クラウドサービスの提供に関する運用状況等の定期的な報告 ・医療機関等の管理者からの問合せ等に対し、一元的に対応できる体制の構築	組織的	監督	A		
	4.1		情報処理事業者の管理者における情報保護責任	4.2	通常運用における責任	(2)	管理責任	運用状況及び管理状況について定期的に報告し、医療機関等から意見又は指摘を受ける	監督		A	経産31p	
	4.1		情報処理事業者の管理者における情報保護責任	4.2	通常運用における責任	(2)	管理責任	電子化された個人情報の保護に一定の知識を有する責任者を定める	組織的		A	経産31p	
4.1			医療機関等の管理者の情報保護責任	(1)	通常運用における責任	③	PDCA	・運用管理状況を定期的に監査 ・問題点を洗い出し、改善すべき点があれば改善	監査等		A	23p	

	4.1		情報処理事業者の管理者における情報保護責任	4.2	通常運用における責任	(3)	PDCA	システムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行った上で医療機関等に報告し、意見又は指摘を受ける	監査等		A	経産31p	
		2.3	クラウドサービス事業者の責任	2.3.1	通常運用における責任	(3)	PDCA	サービス及びセキュリティの向上についての定期的なレビュー結果の報告等	監査等		A	総務27p-	
4.2.1			委託	(1)	通常運用における責任	①	説明責任	受託事業者は医療機関等の管理者に対し説明責任を負うので、その旨を契約事項に含め履行を確保	委託		A	24p	
4.2.1			委託	(1)	通常運用における責任	②	管理責任	受託事業者の管理実態を理解し、監督を適切に行う仕組みを作る必要があり、契約事項に含める	委託	監督	B	24p	
インシデント														
4.1			医療機関等の管理者の情報保護責任	(2)	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	①	説明責任	・医療機関等の管理者はその事態発生を公表 ・原因とそれに対していかなる対処を行うかについて説明	有事		A	23p	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ダンス29p、https://www.ppc.go.jp/files/pdf/iryoukaigo_guidance.pdf） 「個人データの漏えい等の事案が発生した場合等の対応について」（平成２９年個人情報保護委員会告示第１号）に基づき、①事業者内部における報告及び被害の拡大防止、②事実関係の調査及び原因の究明、③影響範囲の特定、④再発防止策の検討及び実施、⑤影響を受ける可能性のある本人への連絡等、⑥事実関係及び再発防止策等の公表の必要な措置
	4.1		情報処理事業者の管理者における情報保護責任	4.3	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	(1)	説明責任	・事態の発生を認識次第、ただちに医療機関等に通知し、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために、協力して情報収集を図る ・発生しうる事態を想定した説明責任の分担を契約事項として含める	有事		A	経産32p	
		2.3	クラウドサービス事業者の責任	2.3.2	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	(1)	説明責任	・緊急時に医療機関等の管理者に対して提供する情報の内容、役割分担等の明確化 ・クラウドサービスの提供状況に関する記録の収集及び緊急時の報告体制の構築 ・媒体及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築 ・緊急時に備えた、 アクセス制御等の手順等の明確化	有事		A	総務28p	
4.1			医療機関等の管理者の情報保護責任	(2)	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	②	善後策を講ずる責任	・原因を追及し明らかにする責任 ・損害を生じさせた場合にはその損害填補責任 ・再発防止策を講ずる責任	有事		A	23p	
	4.1		情報処理事業者の管理者における情報保護責任	4.3	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	(2)	善後策を講ずる責任	・前もって発生しうる事故と考えられる原因を洗い出して対応手順を策定 ・事故に対する緊急対応が完了した後で原因を確定するために、事故発生時の状況を保存あるいは記録する手順、対応過程で行われた作業を記録する手順等も策定 ・確定された原因にもとづき再発防止策を講じる	有事		A	経産32p	
		2.3	クラウドサービス事業者の責任	2.3.2	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	(2)	善後策を講ずる責任	・情報事故（個人情報漏洩等等）が発生した場合の原因追及に必要な情報提供の範囲、条件等の合意、及び情報提供の実施 ・善後策の提案 ・情報事故が発生した場合の損害填補責任に関する合意	有事		A	総務30p	

4.2.1			委託	(1)	通常運用における責任	①	説明責任	委託管理契約で委託先の義務を明記。 特にインシデント発生時の善後策を講ずる責任を医療機関等と受託事業者とでいかに分担するか明記。	委託		B	24p	
4.2.1			委託	(2)	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	①	説明責任	説明責任の分担を契約事項に含める	委託	有事	B	25p	
4.2.1			委託	(2)	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	②	善後策を講ずる責任	・原因追及と再発防止策を優先して協力して行う旨を契約事項に明記 ・場合によっては、受託事業者の責任で原因追及と再発防止策の提案義務を明記 ・損害補てん責任の分担	委託	有事	A	25p	
	4.1		情報処理事業者の管理者における情報保護責任	4.3	事後責任（情報漏えい等のインシデントが発生した際に対処すべき責任）	(3)	再委託先	・再委託先と互いの責任範囲について合意 ・再委託先との契約で上記を明記	委託	有事	A	32p	
委託													
		1.3.2	対象とするクラウドサービス	(1)	想定するクラウドサービスの提供形態	(イ)	複数のクラウド事業者	・クラウド事業者がABCといる場合でも、医療機関等は契約先であるAのガイドライン遵守を確認すればよい ・Aは自社、B、Cのガイドライン遵守を確認。AはBの選択と管理について直接の責任を負い、CについてはBからの報告などに基づく管理責任を負う ・BCも、Aから独立してガイドライン対応する必要がある	委託		A	総務13p-	
		2.3.3	責任分解			(1)	他事業者サービスと自サービスを一体として提供	・Aが自社サービスと、B社IaaSを一体としてサービス提供する場合、Aは医療機関等との間ではクラウドサービス事業者の責任をすべて負う。 ・AもBも独立した立場で、総務ガイドラインの要求事項に対応する ・医療機関とA間の関係同様に、AはBに対し総務ガイドラインへの対応を求める。 ・Bが提供する機能等とA機能等に関する責任分解について取り決める	委託		C	総務30p-	
		2.3.3	責任分解			(2)	医療機関等と契約する他社サービスと自社サービスを組み合わせ	・Aが自社サービスを提供し、医療機関等の指示によりB社IaaSを利用する場合、Aは医療機関等との間ではAが提供するサービスの範囲でクラウドサービス事業者の責任を負う。 ・AもBも独立した立場で、総務ガイドラインの要求事項に対応する ・Bが提供する機能等とA機能等に関する責任分解について取り決める。医療機関等が各社と取り決めるが、ABは必要な対応、情報提供等を行う	委託		C	総務32p-	

		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	(エ)	運用管理規程に基づく文書類の整備	医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。	管理		A	総務44p	
		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	(イ)	クラウドサービスの提供契約についての要求事項	1.守秘義務 ①サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。 2.運用規定等の遵守 ①サービス提供に係る契約において、次項（ウ）1. に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。 3.関係ガイドラインの遵守 ①サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。 ②①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な限り具体的に行う（例えば、総務省が定める「ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針」（平成29年3月31日）に定める事項に準じた情報の提供を行う等）	管理	委託	A	総務40p	情報開示指針は更新されている http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000216.html
	4.4		回線事業者との責任分解点					・インターネットVPN→回線事業者は安全管理上の責任を負わないので、その点のリスクを考慮 ・回線事業者がインターネットVPNを提供→VPN装置含め、回線に起因する障害の責任は回線事業者が負うべき ・閉域網VPN又は専用線→回線上の障害の責任は回線事業者が負うべき（一般には接続用ルータ等の終端機器までは責任範囲）	提供		C	33p	
	4.4		回線事業者との責任分解点					いずれの形態においても、医療機関等と情報処理事業者、回線事業者の責任について、想定される障害等のそれぞれについて契約に明示するなどの対策	提供		A	33p	

		3.2	安全管理に関する要求事項	3.2.9	外部との個人情報の交換	（ウ）	責任分解に関する取り決め	1.通信経路に関する責任分界 ① 通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他 厚生労働省ガイドライン第5版6.11 C 項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 2患者等が閲覧する場合の手続･責任分界 ①サービスにより管理する医療情報を患者等の閲覧に供する場合に、 クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ②医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 ③患者 等 が情報を閲覧する情報システムのセキュリティ に関する説明責任等にお ける クラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関	管理	委託	A	総務120p	
4.3			例示	(2)	リモートアクセス	(b)	リモートメンテナンス	保守の利便性と情報保護の兼ね合いを見極めつつ実施する必要がある。	管理	委託	A	29p	
4.3			例示	(3)	情報が外部に一時的にでも保存される場合			安全管理のほか、情報の保存期間の規定等が必要	管理	委託	A	30p	
	3.3		電子媒体経由の外部保存					・配送事業者については、機密保持契約の締結が可能である、機密情報の配送に特化した配送サービスを提供している、配送状況を利用者が把握する機能を提供している等の条件により事業者を選	提供	委託	A	20p-	
地域医療連携・PHR													

4.2.2			第三者提供					・原則として第三者提供の正当性だけが問題となり、提供後の情報保護責任は提供を受けた第三者に生ずる。但し例外的にずさんなことを知りながら提供した等の場合は、医療機関等の責任が追及される可能性 ・患者に対する関係では、少なくとも情報が受信側に到達するまで、原則として送信側の医療機関等に責任がある。善後策の分担については、情報処理関連事業者及び送信側との間であらかじめ協議し明確にしておくことが望ましい。	提供		B	26p	
4.3			例示	(1)	地域医療連携			①情報処理関連事業者の提供するネットワークを通じて行う場合 ・提供元医療機関等と提供先医療機関等はネットワーク経路における責任分解点を定め、不通時や事故発生時の対処も含めて契約等で合意しておく ・情報処理関連事業者と責任分解点を定め、対処をどの事業者が主体となって行うか明らかにしておく ②医療機関等が独自に接続する場合 ・情報処理関連事業者については、約款に示され	提供		A	27p	
		1.3	対象範囲	1.3.2	クラウドサービス	(2)	医療情報連携ネットワーク	医療情報連携ネットワーク運営主体が、医療情報の取扱いに責任を有する場合には、同主体も総務省ガイドライン上のクラウドサービス事業者になる。一方で、とりまとめや調整のみを行う主体は、クラウドサービス事業者にならない。	提供		C	総務15p-	
		1.3	対象範囲	1.3.2	クラウドサービス	(4)	PHR	医療従事者の取扱いがあれば、患者が管理する医療情報を取り扱うクラウドサービスも、総務省ガイドラインの対象。一方で、患者自らが計測した体温・脈拍数等の医療従事者の取扱いがない情報を扱うクラウドサービスは、総務省ガイドライン	提供		C	総務17p	
		1.3	対象範囲	1.3.2	クラウドサービス	(4)	PHR	PHRサービス事業者で取り扱われる医療情報について、医療機関等の管理責任は及ばないが、患者等の依頼により医療機関等が直接PHRサービス事業者に医療情報を提供する場合は、医療機関等とPHRサービス事業者との間でデータの受け渡しに関する責任分解点を明確にする。通常相手方に到達すると考えられる手法により送信行為を行えば、相手方へ伝達されたとみなすことが適当。	提供		A	総務17, 35p	
個人情報保護方針・第三者認証													
6			情報管理										

6.1			個人情報保護基本方針				最低限	1.個人情報保護に関する方針を策定し、公開していること 2.個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、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。	総論		A	38p-	「個人情報の保護に関する法律についてのガイドライン（通則編）」で記載されている、個人情報保護基本方針に定める項目例としては以下の通り。 「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、
6.2			ISMS					リスクの例がガイドラインに掲載されており、参考になる	管理		C	40p-，経産50p-	
6.2			ISMS				最低限	1.情報システムで扱う情報を全てリストアップしていること 2.リストアップした情報を、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していること 3.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していること 4.リストアップした情報に対してリスク分析を実施していること 5.この分析により得られた脅威に対して、6.3章～6.12章に示す対策を行っていること	管理		A	40p-	
6.2			ISMS				推奨	1.上記の結果を文書化して管理していること。	管理		B	40p-	
	7.1		推奨される認証・認定	7.1.1	ISMS			Pマーク、ISMS等の公正な第三者の認定を取得	総論		A	経産45p	
	7.1		推奨される認証・認定	7.1.1	ISMS	1-3	推奨	・認証取得あるいは更新の際にISMSの安全管理策として、経産ガイドライン7にて提示する安全管理策を盛り込むことが望ましい。 ・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。 ・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）。	総論		B	経産45p-	

		2.5	第三者認証の考え方					・クラウドサービス事業者が情報処理事業者の場合にはPマーク、ISMS等の公正な第三者認証等を取得することが必須 ・これ以外のクラウドサービス事業者においてもPマークが強く求められ、ISMSも望ましい ・第三者認証を取得しても、総務ガイドラインの要求事項をすべて満たすことにはならない	総論		A	総務37p	
外部保存の留意点													
	3.2		ネットワーク利用上の考慮事項					・オープンなネットワーク上のVPNは、適切に運用すること及び医療機関等の合意を得ることを前提として、IpsecにIKEを組み合わせ自動鍵更新を行う設定にする。ネットワーク境界のFW又はVPN装置等により適切なアクセス制御を行うこと。 ・専用線、IP-VPN、オープンなネットワーク上のVPNいずれでも、通信ログ及び通信状況を監視し、異常時に迅速に対処	管理		B	19p	
	3.4		ネットワーク経由の外部保存					管理台帳を活用して、定期的に医療機関等と情報処理事業者間における医療情報電子ファイルの真正性を検証する	提供		B	21p	
	3.4		ネットワーク経由の外部保存					FTPを用いる場合 ・専用回線かVPN等を利用して少なくともネットワークレイヤでの安全対策を施し、パスワード及びデータ漏洩のリスクを低減する ・FTPアクセスログを定期的に検証し、不必要なFTPアクセスが行われていないことを確認するなどの対策を行う	提供		A	23p	
	3.4		ネットワーク経由の外部保存					FTPを用いる場合、単一の安全対策ではなく、ネットワークレイヤでの安全対策に加えて、アプリケーションレイヤにおいてもSFTP、SCP等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用するといった、多重防御を実装	提供		B	23p	
	3.4		ネットワーク経由の外部保存					問題が発見された場合はただちに医療機関等に通知。問題が発見された電子ファイルは原因特定を行うために、削除せずに情報処理装置から隔離したかたちで保管	提供		A	24p	
	3.4		外部保存全般の留意事項					作業手順を医療事業者と合意し、手順書として双方で管理	提供		A	20,21,25p	
	3.4		外部保存全般の留意事項					医療機関等の医療従事者の作業手順 (1)情報処理事業者からの定時報告を確認、検証 (2)不審な点があれば、ただちに確認 情報処理事業者の作業手順 (1)受入れた電子ファイル、払出した電子ファイル、預かっている電子ファイルの数量、発生したイベント等について定期的に確認できる仕組みを構築し医療機関等が確認できるようにする (2)検証手続き中に異常が検出された場合は、直ちに医療機関等に連絡し、適切な事故対応手順を実	提供		A	24p	

	3.4		外部保存全般の留意事項					インターネット経由で転送する場合は、暗号技術を用いて、メッセージの機密性、完全性を確保す	提供		A	24p	
	3.5		アプリケーション入力による外部保存					電子署名の付与が求められる情報については、電子ファイルとして作成してファイルを転送する形をとることが望ましく、その場合には、情報処理事業者にて受け取ったファイルの電子署名を検証	提供		B	25p	
	3.5		アプリケーション入力による外部保存					ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、リスク評価を行い、必要に応じて定期的に脆弱性検査を実施して安全性を確	提供		A	26p	
	3.5		アプリケーション入力による外部保存	3.5.1	データベース利用上の考慮事項			暗号化の検討	提供		A	26p-	
	3.5		アプリケーション入力による外部保存					管理者権限のパスワード管理を厳格に行い、多要素認証などで認証強度を確保。管理者機能を分割しておのおのに別の特権IDを割り当て、それぞれの特権IDの権限を必要最小限とする最小特権の原則を実装することが望ましい	提供		A	27p	
組織的安全管理対策： 組織体制														
6.3			組織的安全管理対策	①	組織体制の整備	1,4	最低限	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。 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。	管理		A	45p-	
		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	（ア）	組織・体制の整備	① サービスの提供についての管理責任を有する責任者を設置する。 ② 情報システム についての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。 ③ サービスの提供に係る情報システムの運用 に関する事務を統括する責任者を設置する。 ④ ①から③に掲げた責任者の任命・ 解任等のルールを策定する。	管理		A	総務40p	
	7.3		組織的安全管理対策			(3)	実施	個人情報保護に関しては、医療機関等の監督の下に行う	管理		A	経産49p	
組織的安全管理対策： 規程等														

6.3			組織的安全管理対策	②	規程等の整備・運用	2,3,5	最低限	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。 5. 運用管理規程等において次の内容を定めること。 (a)理念（基本方針と管理目的の表明） (b)医療機関等の体制 (c)契約書・マニュアル等の文書の管理 (d)リスクに対する予防、発生時の対応の方法 (e)機器を用いる場合は機器の管理 (f)個人情報の記録媒体の管理（保管・授受等）の方法 (g)患者等への説明と同意を得る方法 (h)監査 (i)苦情・質問の受付窓口	管理		A	45p-	
	7.3		組織的安全管理対策			1,2,4,5	実施	・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。 ・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。 ・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。 ・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	管理		A	経産49p	
6.3			組織的安全管理対策	④	PDCA				管理		B	45p	
6.3			組織的安全管理対策	⑤	外部持出に関する規則等				管理		B	45p	
6.3			組織的安全管理対策	⑥	リモートアクセスの管理規程				管理		B	45p	
6.3			組織的安全管理対策	⑦	事故・違反への対処				管理		B	45p	
組織的安全管理対策： 台帳														
6.3			組織的安全管理対策	③	医療情報の取扱い台帳の整備				管理		B	45p	

	7.2		情報資産管理	7.2.1	資産台帳		実施	・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。 ・預託された情報の全てを資産台帳に記録すること。 ・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。 ・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。 ・ 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	管理		A	経産47p	
	7.2		情報資産管理	7.2.1	資産台帳		推奨	・資産台帳等を紙文書として管理する場合に、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。 ・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）	管理		B	経産47p-	
	7.2		情報資産管理	7.2.2	情報の分類		推奨	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	管理		B	経産48p	
	7.2		情報資産管理	7.2.2	情報の分類		実施	・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。 ・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。 ・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。 ・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。 ・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）。 ・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。	管理		A	経産48p	

物理的安全管理対策													
	7.5		物理的安全対策	7.5.1	医療情報処理施設の建物			外部事業者が運用管理するデータセンターに医療情報システムを設置する場合には、経産ガイドライン物理的安全管理策の全てに準拠することは難しい状況が考えられる。その場合には、専有するサーバラック等をセキュリティ領域と考え、不足する物理的安全管理策に相当するその他の対策を施すことが求められる。	管理		C	経産52p	
	7.5		物理的安全対策	7.5.1	医療情報処理施設の建物		実施	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。 ・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。 ・建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入すること。 ・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。	管理		A	経産53p	
		3.2	安全管理に関する要求事項	3.2.2	物理的安全管理対策	（ア）	機器・媒体等の設置場所等	１．施錠管理 ①サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。 ②サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。	管理		A	総務47p	
6.4			物理的安全対策		入退館（室）の管理	2,3	最低限	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でき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得る手段がある場合はこの限りではない。 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。	管理		B	47p	

6.4			物理的安全対策		入退館（室）の管理	1	推奨	防犯カメラ、自動侵入監視装置等を設置すること。	管理		A	経産53p-	
	7.5		物理的安全対策	7.5.2	入退館、入退室等		実施	①情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合 ・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。 ・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。 ・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経産ガイドライン7.6.12参照）。 ・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。 ・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。 ・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	管理		B	経産54p	
	7.5		物理的安全対策	7.5.2	入退館、入退室等		推奨	①情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合 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（PIN40）、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	管理		A	経産54p	

	7.5		物理的安全対策	7.5.2	入退館、入退室等		実施	②外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合 ・データセンターを運営する外部事業者が、上の占有建造物・領域を利用する場合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物理的な不正操作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。 ・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。 ・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。 ・データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。 ・医療情報システムであることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できる	管理		B	経産55p	
	7.5		物理的安全対策	7.5.2	入退館、入退室等		推奨	②外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合 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（PIN40）、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	管理		A	経産55p	
	7.5		物理的安全対策	7.5.2	入退館、入退室等		実施	③ 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合 ・サーバ環境を運営する外部事業者が、上記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	管理		A	47p	

		3.2	安全管理に関する要求事項	3.2.2	物理的安全管理対策	（ア）	機器・媒体等の設置場所等	2.アクセス制御 ①サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ②サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む） は定期的に行う。 ③サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。 ④サービスに供する機器や媒体の設置場所への 不明者の入退を発見するために、入退者に名札等の着用を義務付ける 。 ⑤サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦①～⑥につき、運用管理規程等に規定する。 4.カメラによる監視 ①サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 ②防犯カメラ等の監視映像は記録し、期間を定め	管理		A	総務47p-	
6.4			物理的安全対策		盗難、覗き見等の防止	1,4,5	最低限	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。 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。 覗き見防止の対策を実施すること。	管理		A	経産55p-	
		3.2	安全管理に関する要求事項	3.2.2	物理的安全管理対策	（イ）	運用端末等	①個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等 の対策を行う。 ②運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。	管理		A	総務52p	

	7.5		物理的安全対策	7.5.3	情報処理装置のセキュリティ		実施	・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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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	管理		B	経産56p	
		3.2	安全管理に関する要求事項	3.2.2	物理的安全管理対策	（ウ）	機器・媒体	①個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。 ②個人情報が存在するPC等の重要な機器には、盗難防止用チェーンを取り付ける。 ③受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。	管理		A	総務52p	
	7.5		物理的安全対策	7.5.3	情報処理装置のセキュリティ		推奨	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	管理		A	55p-	
		3.2	安全管理に関する要求事項	3.2.2	物理的安全管理対策	（ア）	機器・媒体等の設置場所等	3.サービスに供する機器や媒体を保存する施設 ①サービスに供する機器や媒体を物理的に保存 するための施設は、災害地震、水害、 落雷、火災等並びにそれに伴う停電等）に耐えうる機能 ・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する 。 ②①の施設を設置する建築物は、サービス仕様適合開示書に基づき、 医療機関等と合意する	管理		A	総務48p	
技術的安全管理対策： 識別・認証													

6.5			技術的安全対策	(1)	利用者の識別・認証	1-4,11	最低限	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．本人の識別・認証にユーザIDとパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 3．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。 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おそれがある場合には、クリアスクリーン等の防止策を講じること。 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。また、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、盗用されたりするおそれがある場合で、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、本人以外が知り得ない方法で再登録を実施すること。	管理		B	57p	
6.5			技術的安全対策	(1)	利用者の識別・認証	2	推奨	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）	管理		B	58p	

		3.2	安全管理に関する要求事項	3.2.4	技術的安全管理対策	（オ）	端末等に表示される医療情報の漏えい	①サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。 ② サービスの運用 ・ 保守端末等を設置している区域 は 監視カメラ等により適切に監視を行う。 ③医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩 防止策について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 ④端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができるようにする。 ⑤医療機関等における利用者端末への④の措置の具体的な適用について、 サービス仕様適合開示書に基づき、医療機関等と合意する。	管理		A	総務69p	
6.5			技術的安全対策	(1)	利用者の識別・認証	4-5	推奨	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。 5. 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又はICカード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように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。	管理		B	48p-	
6.5			技術的安全対策	(1)	利用者の識別・認証			・2要素認証（記憶・生体計測・物理媒体）が望ましく、本ガイドライン第5版公表から約10年後をめどに最低限のガイドラインとすることを想定。 ・2要素認証を採用している場合、必ずしもパスワードの定期的な変更は求められない	管理		A	55p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(ア)	利用者の識別・認証	① 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の 情報システム 利用に係る認証は、2 要素認証以上の認証強度のある方法による。 ② 利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 利用者の認証において、固定式のID ・ パスワードによる認証方式を採用している場合には、固定式のID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成29年5月）から約10年後を目途 に 2 要素 認証 について 厚生労働省ガイドライン 6.5 章 「C. 最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。 ④利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段 ・ 手順を事前に定める。 ⑤代替的手段 ・ 手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。 ⑥代替的手段･手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。 ⑦その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する 。	管理		A	総務60p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(ア)	利用者の識別・認証	①情報システムの利用者を特定し識別できるように、アカウントの発行を行う 複数の利用者による ID の共同利用は行わない。ただし当該 情報システムが他の情報システム を 利用する ためのID non interactive ID ）は除く。 ②利用者のなりすまし等を防止するための認証を行う。 ③利用者には、医療機関等において サービス を利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。 ④情報システムの運用若しくは開発に従事する者又は 管理者権限を有する者に対するIDの発行は必	管理		A	総務58p-	
技術的安全管理対策： 情報の区分管理・アクセス権限管理													

6.5			技術的安全対策	(2)	情報の区分管理とアクセス権限の管理	6	最低限	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。	管理		A	51p-	
6.5			技術的安全対策	(2)	情報の区分管理とアクセス権限の管理			アクセス権限の見直しは人事異動等に合わせて適宜行う必要があり、組織の規程で定めなければならない	管理		B	57p	
6.5			技術的安全対策	(2)	情報の区分管理とアクセス権限の管理	1	推奨	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	管理		A	総務44p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(イ)	情報の区分管理とアクセス権限の管理	1.情報管理区分 ①医療情報とそれ以外の情報を区分できる措置を講じる。 ②医療情報については、情報区分に従ってアクセス制御を行えるようにする。 ③仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。 ④医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 2.権限設定 ①サービスには、医療従事者、関係職種ごとにアクセス権限 ・ 範囲等のアクセス制御が可能な機能を含める。 ②医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。資料の提供に係る条件等については、サービス仕様適合開示書 に基づき、医療機関等と合意する。 3.アクセス対象の設定 ①サービスには、受託する医療情報を患者等ごとに管理できる機能を含める。	管理		A	総務63p-	

		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	(エ)	運用管理規程に基づく文書類の整備	① クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、 並びに アクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定す	管理		A	総務70p	
	7.6		技術的安全対策	7.6.13	アクセス制御方針		実施	(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 (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。	管理		B	経産70p	
	7.6		技術的安全対策	7.6.13	アクセス制御方針		推奨	(1) 作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。 (2) 定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。	管理		A	経産71p	
	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		実施	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。	管理		B	経産71p	

	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		推奨	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。	管理		A	経産71p	
	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		実施	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。 (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。	管理		B	経産71p	
	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		推奨	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	管理		A	経産71p	

	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		実施	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。 (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。 (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。 (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。 (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	管理		B	経産72p	
	7.6		技術的安全対策				推奨	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）、アルファベット及び数字並びに記号を一つ以上含	管理		A	経産72p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	（ア）	利用者の識別・認証	2.本人識別のためにパスワードを設定する時のルール ①本人の識別･認証に、ユーザIDとパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・利用者に対して初期パスワードを発行 した 場合、最初の利用時に そのパスワードを 変更 しないと情報システムにアクセスできないにようにする 。 ・初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める 。 ・パスワードの設定に際しては、複数の文字種（英数字 ・ 大文字 ・ 小文字 ・ 記号等）を用い、また、8 文字以上等、十分に安全な 長さの文字列等から構成されるルールとする。 ②パスワード認証に係る以下のルールを実現する措置を講じる。 ・パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③パスワードには十分な安全性を満たす 有効 期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用している パスワードを使わないよう 特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。	管理		A	総務59p-	
	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		実施	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。 (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。	管理		B	経産73p	

	7.6		技術的安全対策	7.6.14	作業者アクセス及び作業者IDの管理		推奨	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。 (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。 (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。 (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。 (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	管理		A	経産73p	
	7.6		技術的安全対策	7.6.15	作業者の責任及び周知		実施	(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。 (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	管理		A	55p-	
技術的安全管理対策：　アクセスログ													

6.5			技術的安全対策	(3)	アクセスの記録 （アクセスログ）	7-9	最低限	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、並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。 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。 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	管理		A	52p	
6.5			技術的安全対策	(3)	アクセスの記録 （アクセスログ）			・すべてのアクセスログを収集し、定期的に内容をチェックし、不正利用がないことを確認することが必要 ・システム操作に係る業務日誌等を作成し、捜査の記録（操作者及び操作内容等）を管理することでも足りる	管理		A	経産69p	
	7.6		技術的安全対策	7.6.12	ログの取得・監査		実施	（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。 （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。 （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	管理		B	経産69p	

	7.6		技術的安全対策	7.6.12	ログの取得・監査		推奨	(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。 (2)　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、削除記録（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	管理		A	総務44p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(エ)	アクセスログ	1.アクセス記録の取得 ①情報システムへのアクセスを記録し、一定期間保存する 。 ②アクセス記録には、アクセスしたID 、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める。 ③ クセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録 又 はこれに代わる記録について、当該法定年限以上の保存期間を設ける。 ⑤④で定める法定保存年限が経過した医療情報 及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書 に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報 に準じて取り扱う。 ⑥情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセス の 記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。 ⑦⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 2.アクセス記録の保全のための要件 ①アクセス記録が保存されている資源に対し、ア	管理		A	総務66p-	
		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	(エ)	運用管理規程に基づく文書類の整備	② サービスの提供に係る アクセス記録 （外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する 旨を内容とするアクセス管理規程を策定する。	管理		A	56p	
技術的安全管理対策： 不正ソフトウェア・不正アクセス対策														
6.5			技術的安全対策	(4)	不正ソフトウェア対	10	最低限	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。	管理				
6.5			技術的安全対策	(4)	不正ソフトウェア対策			不正ソフトウェア対策ソフトウェアを導入し、パタンファイルを最新化する	管理		B	52p	

6.5			技術的安全対策	(4)	不正ソフトウェア対策			セキュリティパッチの逐次更新、利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等	管理		B	57p	一部A評価もありうる
6.5			技術的安全対策	(5)	ネットワーク上からの不正アクセス	3	推奨	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。	管理		B	52p	
6.5			技術的安全対策	(5)	ネットワーク上からの不正アクセス			・ファイアウォールの単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて外部からの攻撃に対処することが望ましい。システム管理者は、その方式が何をどのように守っているか認識するべき。 ・IDSも検討 ・セキュリティ診断を定期的に実施し、パッチ等の対策を講じることも重要 ・無線LAN やコンセントから不正コンピュータを接続する危険もある ・なりすましの防止を確実に行う ・暗号化等による情報漏えい対策も必要	管理		A	経産59p	

	7.6		技術的安全対策	7.6.3	悪意のあるコード		実施	医療情報システムに悪意のあるコードが混入しないよう、施設内のサーバ及び端末にて以下の対策を施す必要がある。アプライアンスサーバのように、サーバ上で悪意のあるコード対策ソフトウェアを稼動させることができない場合には、サーバと他機器を接続するネットワーク経路上で同様の悪意のあるコード対策を行うこと。 ・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。 ・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 ・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	管理		A	経産61p-	

	7.6		技術的安全対策	7.6.6	ネットワークセキュリティ		実施	・セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。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ウ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。 ・セキュリティゲートウェイでは、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）。 ・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。 ・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。 ・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。 ・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	管理		B	経産64p	
	7.6		技術的安全対策	7.6.6	ネットワークセキュリティ		推奨	・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。 ・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	管理		A	57p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(カ)	情報漏えい対策等	①外部のネットワークと医療情報を格納する機器との接続に際しては、セキュリティゲート ウ ェイ ネットワーク境界に設置したファイアウォール、ルータ等 を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。 ②医療機関等との接続ネットワーク境界には、侵入検知システムIDS 、侵入防止システムIPS 等を導入してネットワーク上の不正なイベント を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③侵入検知システム等が、常に最新の攻撃 ・ 不正アクセスに対応可能なように、シグネチャ ・ 検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。 ④ホスティングの利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置	管理		A	総務70p	
6.5			技術的安全対策	(6)	医療等分野におけるIoT機器の利用	13	最低限	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	管理		B	58p	一部A評価もありうる
6.5			技術的安全対策	(6)	医療等分野におけるIoT機器の利用	7	推奨	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。	管理		B	53p-	

6.5			技術的安全対策	(6)	医療等分野におけるIoT機器の利用			・「IoTセキュリティガイドライン」が参考になる ・リスク分析を行い、その取扱いにかかる運用管理規程を定める ・患者への説明、リスクに関する同意取得 ・のちに脆弱性が発見された場合にサービス提供に支障が生じないよう対策を講じる ・使用を終えた機器等は電源を切り接続を遮断する等	管理		A	55p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(コ)	IoT	①IoT機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、 サービス仕様適合開示書に基づき、 医療機関等と合意する。 ②IoT機器の利用を含むサービスを提供する場合、IoT 機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。 ③IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。	管理		A	総務79p	
6.5			技術的安全対策	(7)	その他	5	最低限	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	管理		A	56p-	
6.5			技術的安全対策	(7)	その他	12	最低限	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行うこと。 (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。	管理		B	55p	
6.5			技術的安全対策	(7)	その他			・無線LANでは通信遮断等もありうるので、可用性確保 ・無線電波により重大な影響を被るおそれのある機器等の周辺利用に注意 ・電力線搬送通信（PLC）による医療機器に対する安全性に注意	管理		B	58p	

6.5			技術的安全対策	(7)	その他	6	推奨	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	管理		A	経産65p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(コ)	無線LAN	医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、 医療機関等と合意する。	管理		A	総務79p	
技術的安全管理対策： 構築・試験・保守・運用													
	7.6		技術的安全対策	7.6.1	情報処理装置及びソフトウェアの保守		実施	情報処理装置の更新、補修などのために文書化された保守手順を確立し、適切に運用しなければならない。以下の管理策を適用すること。 ・保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。 ・変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。 ・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間、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。 ・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。 ・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。 ・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。 ・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。 ・潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。 ・修正パッチの適用前にパッチが改ざんされてい	管理		B	経産59p-	

	7.6		技術的安全対策	7.6.1	情報処理装置及びソフトウェアの保守		推奨	・変更手順に含まれる事項には次のようなものが考えられる。 ●変更についての影響が及ぶ関係者への通知プロセス ●装置の変更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、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等） ●申請承認プロセス ●変更試験プロセス ●変更作業に支障が発生した場合の復旧手順 ●変更終了確認プロセス ●変更に伴う影響を監視するプロセス、等。	管理		A	経産60p	
6.8			情報システムの改造と保守	①	保守会社の守秘義務	最低限	1,6	・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 ・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	委託	管理	B	63 p	
6.8			情報システムの改造と保守	①	保守会社の守秘義務	推奨	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	委託	管理	A	62p-	
6.8			情報システムの改造と保守	②	保守要員の登録管理	最低限	2-4	・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。 ・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 ・保守要員の離職や担当替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	委託	管理	A	62p-	
6.8			情報システムの改造と保守	③	作業計画報告の管理	最低限	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	委託	管理	A	経産77p	
	7.9		医療情報システムの改造と保守				実施	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	委託	管理	B	経産77p	

	7.9		医療情報システムの改造と保守				推奨	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。	委託	管理	A	62p-	
6.8			情報システムの改造と保守	④	監督等	最低限	7-9	・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 ・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ともに、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 ・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の責任で同等の義務を課すこと。	委託	管理	B	63 p	
6.8			情報システムの改造と保守	④	監督等	推奨	1,2,4,5	・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 ・保守作業時には医療機関等の関係者立会いの下で行うこと ・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 ・保守作業に関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	委託	管理	C	65p	
		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	（ア）	アカウント管理	1.保守用のアカウント ① 情報システムの保守に従事する者 及び 管理者権限を有する者が、その業務の目的で 当該 情報システム にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。 ② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。 2.保守用のアカウントの管理 ①情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが 漏洩	管理		A	総務90p	

		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	（イ）	保守実施	1.リモートメンテナンス ①リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システム への不正な侵入が生じないよう安全管理措置を講じる。 ②リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム 管理者はその内容を速やかに確認する。 ③サービス提供に必要な 情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、 医療機関等と合意する。 2.ログによる保守結果のレビュー ①情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。 ②取得した 操作ログ等により、アクセスされた医療情報 についての状況をレビューする。 3.医療機関等内における保守対応 ①情報システムの保守業務を医療機関等の施設内で行う際の対応について 、サービス仕様適合開示書に基づき、医療機関等と合意する。 4.保守業務の実施報告 ①情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。 事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ②①における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場	管理		A	総務91p	
		3.2	安全管理に関する要求事項	3.2.9	外部との個人情報の交換	（イ）	保守における通信上の安全管理対策	リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。	管理	委託	A	総務120p	

		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	（ウ）	保守に用いるデータ	1.保守で用いるデータ ① 情報システムの動作確認に際しては 、原則 として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ② 情報システムの動作確認に際し、受託した 個人情報 を含むデータをやむを得ず使用する場合には、３．２．４で示す守秘義務が課された要員・委託先等により動作確認を行う旨を含めた手順を定める。 ③ 情報システムの動作確認に際し、受託した個人情報をやむを得ず使用する場合 について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 2.保守目的 での医療情報の持ち出し ①医療情報を格納する機器等を、保守（例えば機器の 修理 等）の目的で、医療機関等 又は クラウドサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。 ②①で定め る 手順 及び情報の提供条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。	管理		A	総務93p	

		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	(エ)	整合性・継続性確保	1.データ項目の標準形式の採用 ①診療録等のデータ項目で、 厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。 ②厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式 とし、サービス仕様適合開示書に基づき、医療機関等と合意する。 2.レコード管理方法等 ①医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える。 ②①に示す機能等を備えることが困難な場合の 情報システム 更新 ・ 移行の手順について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 3.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 ①データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。 ②①の結果、サービスの利用に影響があると認められ る 場合には、医療機関等が対応を図る ために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。 ③②は、他の情報システムとのデータ連携等を考慮して行う。 医療機関等に対する互換性確保に係	管理		A	総務94p	
		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	(オ)	体制・再委託	1.保守体制の変更 ①情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。 2.再委託先の体制 ① 情報システムの保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。 ② ①の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。	管理		A	総務96p	
		3.2	安全管理に関する要求事項	3.2.6	情報システムの改造と保守	(エ)			管理		A	総務93p	

	7.6		技術的安全対策	7.6.2	開発施設、試験施設と運用施設の分離		実施	医療情報システムの開発施設及び試験施設と運用施設は分離されていなくてはならない。開発主体が情報処理事業者あるいは外部事業者、どちらの場合においても以下の措置を行うこと。 ・情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。 ・ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行うこと。 ・開発施設では悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には経産ガイドライン7.6.3に従うこと。 ・不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること ・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。 ・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	管理		B	経産60p	
	7.6		技術的安全対策	7.6.2	開発施設、試験施設と運用施設の分離		推奨	ソフトウェアに悪意のあるコードが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい	管理		A	経産61p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	（カ）	情報漏えい対策等	①情報システムの構築に際しては 、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。 ②ウイルス対策ソフトのパターン定義ファイル を常に最新のものに更新する。 ③情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。 ④サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。 ⑤情報システムの脆弱性に関する情報は、JPCERT/CC、NISC、IPA等の情報源から、定期的及び必	管理		A	総務70p	
	7.6		技術的安全対策	7.6.4	ウェブブラウザ		実施	・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 ・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）。 ・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経産ガイドライン7.6.3に即して検査されること。	管理		B	経産62p	
	7.6		技術的安全対策	7.6.4	ウェブブラウザ		推奨	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	管理		A	経産62p	
	7.6		技術的安全対策	7.6.9	セキュリティ要求事項		実施	(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。 (3) 業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。 (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。	管理		A	経産67p-	

	7.6		技術的安全対策	7.6.10	アプリケーション		実施	(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。 (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。 (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	管理		B	経産68p	
	7.6		技術的安全対策	7.6.10	アプリケーション		推奨	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。	管理		A	経産68p	
	7.6		技術的安全対策	7.6.11	暗号		実施	(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。	管理		B	経産68p	

	7.6		技術的安全対策	7.6.11	暗号		推奨	(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。 (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。	管理		A	59p-	
技術的安全管理対策：　第三者提供サービス（監視、保守点検作業、清掃作業等）													
	7.6		技術的安全対策	7.6.5	第三者提供サービス（監視、保守点検作業、清掃作業等）		実施	・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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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、厚労ガイドライン第4.1 版6.8 章C 項の管理策を実施する。	管理		B	経産62p	
	7.6		技術的安全対策	7.6.5	第三者提供サービス		推奨	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。	管理		A	経産63p-	
技術的安全管理対策：　電子媒体													
	3.1		電子媒体の選択についての考慮事項					・microSD等の小型半導体メモリは、衣服などのわずかな隙間にも隠すことができるため、原則として使用できないように配慮 ・必要な場合には、使用前に不要データが書き込まれていないことを確認し、使用後に全データを削除。利用時間及び移動範囲を最小にする等の管理を行う。	管理		B	18p	

	7.6		技術的安全対策	7.6.7	電子媒体		実施	(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。 （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。 （5） 電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管すること。 （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。 （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。	管理		B	経産65p-	
	7.6		技術的安全対策	7.6.7	電子媒体		推奨	（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。 （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。	管理		A	経産66p	
技術的安全管理対策： 医療機関等と情報処理事業者間の情報交換														

	7.6		技術的安全対策	7.6.8	医療機関等と情報処理事業者間の情報交換		実施	(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 (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。 ●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）。 ●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。 (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づいて信頼できる配送業者を選択すること。 ●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	管理	委託	A	経産67p	
人的安全管理対策													
6.6			人的安全対策	(1)	従業者			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当たって、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個人情報の安全管理に関する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	管理	監督	B	60p	
6.6			人的安全対策	(1)	従業者			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	管理	監督	A	60p	

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	最低限	1,2	1．医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ①受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること ②保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ③清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 ④委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。 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。	委託	監督	A	経産74p	

	7.7		人的安全対策				実施	(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。 (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。 (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。 (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。	管理	監督	B	経産74p	
	7.7		人的安全対策				推奨	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。	管理	監督	A	61p	

		3.2	安全管理に関する要求事項	3.2.4	人的安全管理対策	（ア）	従業者等に対する守秘義務等	1.就業開始時における対応 ①サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。 2.就業時における教育等 ①サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育 ・ 訓練を行う。 ②この教育 ・ 訓練は 就業開始時及び就業後定期的に行う。 3.退職後の守秘義務等 ①サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。 ②サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含むに返却を求め、システム管理者が返却されたことを確認する。 ③サービスの提供に従事する要員の退職時又は 契約終了時以降の守秘義務について、上記2における教育･訓練に含める。 4.守秘義務違反者への対応措置 ① 上記 1. 3. に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。 5.従業者等への教育状況 ・ 守秘義務等の状況 ①サービスの提供に従事する要員に対する教育 ・	管理		A	総務82p	
		3.2	安全管理に関する要求事項	3.2.4	人的安全管理対策	（イ）	再委託先	①情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。 ② 再委託先には、自社と同等の個人情報保護指針等を遵守させる。 ③ 再委託に係る契約に、委託業務に係る守秘義務を含める。 ④ 再委託先に対して、委託先要員に自社と同等の	管理	委託	A	総務83p	
情報の破棄													

6.7			情報の破棄			最低限	1-4	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. 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。 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	管理	委託	A	経産76p	
	7.8		情報の破棄				実施	(1) CD-R 等の廃棄については「7.6.7 電子媒体の取扱」参照 (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 (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。	廃棄		A	経産56p-	
	7.5		物理的安全対策	7.5.4	情報処理装置の廃棄及び再利用		実施	・ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。 ・サーバ等のBIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。 ・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。 ・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。	廃棄		B	経産57p	

	7.5		物理的安全対策	7.5.4	情報処理装置の廃棄及び再利用		推奨	・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 ・ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施する	廃棄		A	62p-	
		3.2	安全管理に関する要求事項	3.2.5	情報の破棄			1.情報の破棄の保証 ① サービスに供する情報を格納する機器、媒体等を破棄する手順に、不可逆的な破壊 ・ 抹消等 により元のデータを復元できなくする措置を含める。 ②情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法 （電磁記録媒体の消磁 ・ 物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。 ③①で講じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書 に基づき、医療機関等と合意する 。 2.情報破棄手順の文書化 ①運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと 。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置 事前に破棄の基準等を告知する等）。 ② 情報の破棄手順について、サービス仕様適合開	廃棄		A	総務86p	
情報及び機器持出													
6.9			情報及び機器持出					「スマートフォン・クラウドセキュリティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～」（総務省；平成24年6月）が参考になる	管理		A	66p	

6.9			情報及び機器持出			最低限	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	管理		A	66p	
6.9			情報及び機器持出			最低限	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	管理		A	経産57p, 総務101p	
	7.5		物理的安全対策	7.5.5	情報処理装置の外部持出		実施	・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。 ・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。	管理		B	経産57p-	
							推奨	・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。 ・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	管理		A	66p	
6.9			情報及び機器持出			最低限	3	情報を格納した可搬媒体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	管理		A	66p	
6.9			情報及び機器持出			最低限	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	管理		A	66p	
6.9			情報及び機器持出			最低限	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若しくは情報機器の所在について台帳を用いる等して把握すること	管理		B	67p	
6.9			情報及び機器持出			推奨	3	情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること	管理		A	66p	
6.9			情報及び機器持出			最低限	6	情報機器に対して起動パスワード等を設定すること。設定に当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	管理		B	67p	
6.9			情報及び機器持出			推奨	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	管理		A	66p	
6.9			情報及び機器持出			最低限	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	管理		A	66p	

6.9			情報及び機器持出			最低限	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。	管理		B	65p	
6.9			情報及び機器持出					自動的に公衆無線LANに接続してしまう端末も存在するので、業務アプリ起動時にVPN接続を確立しない場合は、公衆無線LANへの自動接続機能を切る必要がある	管理		A	66p	
6.9			情報及び機器持出			最低限	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	管理		B	65p	
6.9			情報及び機器持出					OSのメモリ管理機能で、メモリを隔離して他のアプリの影響を受けないアプリが構築可能な場合は、確実にメモリ隔離ができることを確認することが必要である	管理		A	66p	
6.9			情報及び機器持出			最低限	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	管理		A	66p	
6.9			情報及び機器持出			推奨	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	管理		B	67p	
6.9			情報及び機器持出			推奨	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。	管理		A	71p	
		3.2	安全管理に関する要求事項	3.2.7	情報・機器の持出	（イ）	台帳管理	情報を格納する機器・媒体等については台帳管理等を行い、定期的に所在確認を行う。	管理		A	総務103p	

		3.2	安全管理に関する要求事項	3.2.7	情報・機器の持出	（ウ）	持出の漏えい対策	1.起動パスワードの設定 ① サービスに供する機器等については、起動パスワードの設定を行う。 ② 起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。 ③ サービスに関する情報を格納する情報機器 へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。 2.機器を持ち出す場合の手順 ①サービスに関する情報を格納する機器 ・ 媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる 、パスワードを設定する 等 の 事項を含める。 3.持ち出し機器等におけるアプリケーション ①サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。 ②サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。 4.BYODへの対応 ①サービスの提供に係る目的（開発、保守、運用含むで従業員等の個人所有の機器を利用することは禁止する。 ②利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する。なお具体	管理		A	総務104p	
6.10			災害・サイバー攻撃等の非常時の対応	(1)	非常時における事業継続計画	最低限	1-2	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 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	管理	有事	A	経産79p	
事業継続計画													

	7.10		事業継続計画	7.10.1	要求事項の識別		実施	(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。 (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。 (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	管理	有事	A	経産79p	
	7.10		事業継続計画	7.10.2	事業継続計画の立案・レビュー		実施	(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。	管理	有事	B	経産80p	

	7.10		事業継続計画	7.10.2	事業継続計画の立案・レビュー		推奨	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 ・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） ・所管官庁への連絡体制等	管理	有事	A	71p	所管省庁への連絡よりも、本文中に記されているネットワークの切断・隔離の方が最優先ではないか？なぜこれが最低限求められる事項なのか？所管官庁に連絡したら、所管間著がネットワーク切断してくれるわけ
6.10			災害・サイバー攻撃等の非常時の対応	(2)	非常時使用への対応	最低限	3	・「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て、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。 ・ 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	管理	有事	A	71p	

		3.2	安全管理に関する要求事項	3.2.8	災害等の非常時の対応	（イ）	災害等の非常時の対応	1.BCP等の策定 ①サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ②①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。 ③①で策定したBCP及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、医療機関等と合意する 。 2非常時のサービスの運用 ①非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 ②非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。 ③非常時に用いる利用者アカウントが利用された場合 システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。 ④非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。 4サービス回復後のデータ整合性の確保 ①非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規	管理		A	総務109p	
6.10			災害・サイバー攻撃等の非常時の対応	(3)	サイバー攻撃	最低限	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、“非常時”と判断した上で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	管理	有事	B	70p-	
6.10			災害・サイバー攻撃等の非常時の対応	(3)	サイバー攻撃			・攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断 ・他の機器への感染拡大の防止や情報漏えいの抑止のための当該感染機器の隔離 ・他の機器への波及の調査等被害の確認のための業務システムの停止 ・マルウェア等に感染した場合、バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを取得することが望ましい）	管理	有事	A	72p	

		3.2	安全管理に関する要求事項	3.2.8	災害等の非常時の対応	（イ）3	災害等の非常時の対応	①サイバー攻撃等により、サービスの提供 に 支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。 ②①の場合において、サービスに生じている障害の 状況 及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。 ③①の場合において、医療機関等が行う必要のある所管官庁への連絡・ 報告のために提供する 資料の範囲、条件等について、サービス仕様適合開示書に基づき、 医療機関と合意する。 ④③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ ストレージ等は国内法の 執行 が及ぶ場所に設置する。	管理		A	総務109p	
外部との個人情報の交換													
6.11			外部との個人情報の交換					・「送付すべき相手に」「正しい内容を」「内容を盗み見されない方法で」送付 ・送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威からの防御 ・情報を伝送するまでの医療情報の管理責任は送	提供		A	73p	
6.11			外部との個人情報の交換	B-1	医療機関等の留意事項	①	盗聴への対応	医療情報の暗号化（オブジェクト・セキュリティ）	提供		B	73p	
6.11			外部との個人情報の交換	B-1	医療機関等の留意事項	①	盗聴への対応	少なくとも、医療機関等の設備から情報が送出される段階で暗号化されていることが望ましい。リモートログインによる保守時も同様であり、保守委託事業者等に確認・監督する	提供		B	73p-	
6.11			外部との個人情報の交換	B-1	医療機関等の留意事項	②	改ざんへの対応	暗号化、電子署名等	提供		A	74p	
6.11			外部との個人情報の交換	B-1	医療機関等の留意事項	③	なりすましへの対応	送信先が確かに意図した相手であるかを確認 例：公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等、電子署名	提供		C	74p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ			・通信経路上での脅威への対応であるチャネル・セキュリティ ・責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理 ・ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、情報を受信する機関の外部ネットワーク接続点までや、業務の必要性から並びに患者からのアクセスを許可する等、外部から医療機関等の情報システムにアクセスする接続点までのことを指し、医療機関等の内部で構成されるLANは対象とならな	提供		A	74,75p	

6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ			・交換しようとする情報の機密性を整理し、コスト・運用に対して適切なネットワークを選択する。例えば予約サイトに過度のセキュリティ対策は不要。 ・提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定。選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要	提供				
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ			回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合は、管理責任の大部分を事業者に委託可	提供		A	75p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ			たとえば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式等、回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合は、導入したネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識を持たない者が安易にネットワークを構築して医療情報等を脅威にさらさないように、万全の対策を実施。情報の送信元・送信先に導入されるネットワーク接続機器に加え、医療機関等内に設置されている情報端末、当該端末に導入されている機能及び端末の利用者等を確実に確認する手段を確立する必要がある。また、情報をやり取りする機関同士での情報の取扱いに関する契約の締結、（脅威が発生した際に備えて）通信事業者にネットワーク経路上のセキュリティを委託する場合よりも厳密な運用管理	提供				
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ				提供				
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ				提供		A	76, 78p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	I	クローズドネットワーク	・暗号化 ・ウイルス対策ソフトのパターン定義ファイルやOSのセキュリティ・パッチ等を適切に適用し、コンピュータシステムの安全性確保に配慮	提供		A	78p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ			異なる通信事業者のクローズドなネットワーク同士が接続点を介して相互に接続されている形態も存在。一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとはいえない。電気通信事業法があり、万一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。	提供		C	76p	

6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	①	専用線	・専用線接続とは、2地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続。通信事業者によってネットワークの品質と通信速度（以下「帯域」という。）等が保証 ・ネットワークの接続形態としては拡張性が乏しく、高コスト	提供		C	77p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	②	公衆網	・ISDN（Integrated Services Digital Network）やダイアルアップ接続等、交換機を介した公衆回線を使って接続する接続形態 ・ISPを介さず、情報の送信元が送信先に電話番号を指定して直接接続する方式 ・ネットワーク接続を確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる ・拡張性が乏しく、通信速度が遅いため、大量の情報若しくは画像等の容量の大きな情報の送信には不向き	提供		C	77p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	③	閉域IP通信網	通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式、IP-VPN	提供		A	79p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	Ⅱ	オープンなネットワーク	・「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策 ・医療情報そのものの暗号化	提供		C	79p	
6.11			外部との個人情報の交換	B-2	ネットワークセキュリティ	Ⅱ	オープンなネットワーク	・回線事業者とオンラインサービス提供事業者が、ネットワーク経路上のセキュリティを担保した形態でサービス提供することも。この場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できるため、契約等で管理責任の分界点を明確にした上で利用することも可能 ・医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医 療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関 等の判断で導入	提供		C	82p-	

		3.2	安全管理に関する要求事項	3.2.9	外部との個人情報の交換	(ア)	ネットワーク	1.ネットワーク経路における全般的な安全管理対策 ① ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等 から保護するために必要な措置（情報交換の実施基準 ・ 手順等の整備、通信の暗号化 等）を行う 。 ② アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置 サーバ証明書 の導入等 ）を行う。 ③ 経路の安全性確保のため、 IPSec + IKE への対応や閉域ネットワークへの対応等及びその条件等について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する 防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 ⑤ 医療機関等がチャネル・ セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、 医療機関等と合意する。 2.医療機関等からのネットワーク経路の確認 ①医療機関等からクラウドサービス事業者までのネットワークにおいて、 医療機関等の送受信の拠点の出入り口･使用機器･使用機器上の機能単位 ・利用者等の必要な単位で経路の確認を行う。 ②①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相	管理		A	総務 115p-	
6.11			外部との個人情報の交換	Ⅲ	モバイル端末等の利用			公衆網の経由、インターネットの経由、閉域ネットワークの経由どのパターンにあたるかの例示解説あり。自分がやろうとしている接続が、どの形態に当たり、どのようなリスクがあるかを理解す	提供		A	87p-	
6.11			外部との個人情報の交換			1	最低限	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。 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行う。 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行う。 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挙げられる。 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。	提供		A	88p	

6.11			外部との個人情報の交換			2	最低限	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。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。 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	提供		A	88p	
6.11			外部との個人情報の交換			3	最低限	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行う。6.5参照	提供		A	88p	
6.11			外部との個人情報の交換			4	最低限	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。 安全性が確認できる機器とは、例えば、S015408 で規定されるセキュリティターゲット若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。	提供		A	88p	
6.11			外部との個人情報の交換			5	最低限	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。例えば、 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。暗号化の鍵については電子政府推奨暗号のものを使用	提供		A	88p	
6.11			外部との個人情報の交換			6	最低限	次の事項について、医療機関等、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の責任分界点、責任の所在を契約書等で明確にする。 ・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又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又は送信先の医療機関等が	提供	委託	A	89p	

6.11			外部との個人情報の交換			6	最低限	医療機関内で次の事項において契約や運用管理規程等で定める ・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）	提供		A	89p	
6.11			外部との個人情報の交換			7	最低限	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。6.8も参照。	提供		A	89p	
6.11			外部との個人情報の交換			8	最低限	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。また、最低限1及び4を満たしているこ	提供		A	89p	
6.11			外部との個人情報の交換			9	最低限	・患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI 個人認証等の技術を用いた対策を実施する。 ・患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含め	提供		A	89, 80p	
6.11			外部との個人情報の交換			10	最低限	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。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。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。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、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃からの防護について、適切な対策を実施。 http://www.hispro.or.jp/open/pdf/2009090nRece	提供		B	90p	

6.11			外部との個人情報の交換			1	推奨	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ともに、運用等の要件を設定する	提供		A	91p-	
6.12		3.2.10	電子署名					(割愛)	管理				
7			電子保存の要求事項										
	6		電子保存の要求事項								C	95p,経産40p	
真正性													
7.1	6.1		真正性					・真正性とは、正当な権限において作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であること。混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすること。 ・完全性が近いがそれ以上の概念	管理		B	経産40p	
								医療情報を作成する医療従事者及び医療機関等が真正性を確保することができるよう、情報記録者が誰であるのかについて電磁的記録として認識できるよう、文書フォーマット等について医療機関等と十分な合意を形成しておくべき	管理		A	95p	
7.1			真正性					ネットワークを通じて外部に保存を行う場合、委託元の医療機関等から委託先の外部保存施設への転送途中で、診療録等が書換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。 従って、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は、医療機関等に保存する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意。	管理		A	96p	

7.1			真正性	B-1	虚偽入力、書換え、消去及び混同を防止	(1)		1.　情報の入力や記録の確定に係る作業の手順等を運用管理規程に記載すること。 2.　情報の入力者、及び入力者と確定者が異なる場合はその両者（以下「入力者及び確定者」という。）が明確で、いつでも確認できること。 3.　入力者及び確定者の識別・認証を確実に行うこと。すなわち、なりすまし等が行えないような運用操作環境を整備すること。 4.　入力者やシステムを操作できる者の権限に応じてアクセスできる情報を制限すること。 5.　入力者及び確定者が行った操作に関して、いつ、誰が、どこで、どの情報に対して、どんな操作を行ったのかが記録され、必要に応じて、操作記録に対して医療機関等が定めた運用管理規程に準拠した適正な利用であることが監査されること。 6.　確定された情報は、確定者によって確定操作が実施されたことが医療機関等で定めた運用管理規程に準拠して監査できること。 7.　確定され保存された情報は、運用管理規程で定めた保存期間内は履歴を残さないで改変、消去ができないようにすること。 8.　システムの改造や保守等で診療録等にアクセスされる可能性がある場合には、真正性確保に留	管理		A	経産40p-	
	6.1		真正性					・情報の受入れ時に正しい情報であることを確認する。このためには医療機関等側で情報を生成した際に、例えば電子署名を付与するなど。情報を受入れた情報処理事業者は、付与された電子署名を検証するなど、真正性を検証することで情報が通信路上で変更されていないことを確認できる。 ・受入れ後はハードディスクや光学ディスク等の電子媒体に情報を書き込んで保存する。情報を保存した電子媒体について、認可されていない着脱、持出が行われていないことを保証するため、定期的に検査を行う。また、電子媒体上の情報に対して、認可されていない書き込み、削除が行われないように、アカウント管理、アクセス権限管理を行い、定期的に電子署名を検証する等の作業により改ざんの検出を行う。 ・医療機関等の要請により情報を提供する際にも電子署名を検証等の作業により改ざんの検出を行い、正しく元の情報を提供する。 ・情報の廃棄に関しては医療機関等からの依頼により行うことであり、処理が厳正に執り行われた	管理		A	99p-	

7.1			真正性	B-2	作成の責任の所在を明確に	(1)	入力者及び確定者の識別・認証	電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 1.　入力者及び確定者を正しく識別し、認証を行うこと。 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、権限のある入力者以外による作成、追記、変更を防止すること。 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。 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1.　装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、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。 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。	管理		A	100p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(イ)	利用者の識別・認証	1.PC等の汎用入力端末により記録が作成される場合 ①ｅ文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、 以下の事項 について、サービス仕様適合開示書 に基づき、 医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様 2.臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 ①ｅ文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等 、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・サービスとの連携におけるインタフェースの構	管理		A	総務64p	

7.1			真正性	B-2	作成の責任の所在を明確に	(2)	記録の確定手順の確立と、識別情報の記録	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。 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。 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。 4.　確定された記録が、故意による虚偽入力、書換え、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。 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。 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。 b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若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、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、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。	管理		A	101p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	（ウ）	真正性の確保	1.PC等の汎用入力端末により記録が作成される場合 ①ｅ文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、 以下の事項について、サービス仕様適合開示書 に基づき、 医療機関等と合意する。 ・確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時に関する仕様・入力された内容についての記録確定前における確認の可否等についての仕様 ・記録の確定権限に関する仕様 ・確定した記録の追記・ 削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様	管理		A	総務65p	

7.1			真正性	B-2	作成の責任の所在を明確に	(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わせることができること。 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。	管理		A	101p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(ウ)	真正性の確保	1.更新履歴比較機能 ①真正性が求められる医療情報を取り扱うサービスには 、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は 更新履歴等が保存される等、更新前後の内容を照らし合せることができる 機能を含める。 2.更新順序識別機能 ①真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。	管理		A	総務65p	
7.1			真正性	B-2	作成の責任の所在を明確に	(4)	代行入力の承認機能	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。 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、その代行入力の都度記録されること。 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。	管理		A	101p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(ウ)	真正性の確保	①真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 ②真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等） を 記録する機能を含める。 ③真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作承認）に関する機	管理		A	総務66p	

7.1			真正性	B-2	作成の責任の所在を明確に	(5)	機器・ソフトウェアの品質管理	1.　システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。 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.　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。 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。	管理		A	101p-	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(ク)	品質管理	1.情報システムに関するドキュメント作成 ①情報システムにおける機器及びソフトウェアの構成図を作成する。 ②情報システムのネットワーク構成図を作成する。 ③①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。 ④情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。 ⑤①④で策定した資料等を 医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を医療機関等と合意する。 2.品質管理に関する運用 ①サービスに供する機器 及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。 ②サービスに供する機器 及び ソフトウェアの品質管理に関する教育を従業員等に対して行う。 ③サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。 ④システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含	管理		A	総務76p	

7.1			真正性				ネットワークを通じて医療機関等の外部に保存する場	(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、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。 (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。 (3)　リモートログイン機能を制限すること 保守目的等、どうしても必要な場合を除いて行うことができないように、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。	管理		C	103p，経産42p	
見読性													
7.2	6.2		見読性					・見読性とは、電子媒体に保存された内容を診療」「患者への説明」「監査」「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で、肉眼で見読可能な状態にできること ・可用性に近いがそれ以上の概念	管理		A	104p	
7.2			見読性			(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、患者ごとの情報の全ての所在が日常的に管理されていること	管理		A	104p	
7.2			見読性			(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。	管理		A	104p	
7.2			見読性			(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若しくは書面に表示できること	管理		A	104p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	(キ)	応答時間	医療機関等がサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、サービス仕様適合開示書に基づき、 医療機関等と合意する。	管理		A	総務73p	
7.2			見読性			(4)	システム障害対策としての冗長性確保	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（障害の発生時にもシステム全 体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備 し、運用すること）を行う又は代替的な見読化手段を用意	管理		A	42p	

		3.2	安全管理に関する要求事項	3.2.8	災害等の非常時の対応	（ア）	障害時における見読性確保	1.障害時の責任分界 ①障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。 2.医療機関への情報提供 ①医療情報を医療機関等に保存する場合に、 障害時における見読性確保のため に 医療機関等側で講じうる方策に関する情報提供について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 3.外部ファイル等の出力 ①医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、 医療機関等と合意する 。 4.遠隔地のバックアップに関する見読性 ①医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、 サービス仕様適合開示書に基づき、医療機関等と合意する。 5.見読性の確保の支援機能 ①緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能 例えば画面の印刷機能、ファイルダウンロードの機能等をサービスに含めること 及 びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基	管理		A	総務108p	

	6.2		見読性					・見読可能となるまでの時間的要求について、医療機関等と合意しておく ・ネットワークの可用性について十分に検討。特にデータ容量が大きい高精細デジタル画像である医用画像（レントゲンデータ等）を扱う場 合は、ネットワークの回線容量について配慮 ・重要インフラの一部に相当する意識を持ち、適切な事業継続計画を策定する ・システムの更新、アプリケーションの変更等に伴い、電子保存された医療情報の読み出しに関する互換性を失わないように配慮 ・情報処理事業者側の経営上の判断または経済的理由等から、サービス提供を終了せざるを得ない状況Deも、医療機関等の業務継続に悪影響を与えないよう、預託データの速やかな返却、他情報処理事業者へのサービス移管を可能とする配慮 ・アプリケーション入力の場合は厚労医療情報安全管理ガイドラインの「5」に示されている、基本データセット、標準的な用語集、コードセット、データ交換のための国際的な標準規格について、十分に理解し、実装するアプリケーションにおいて提供サービスの可用性、データの互換性の確保に務める	管理		B	105p	

7.2			見読性				推奨	【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。 (2)　見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。 (3)　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。 【ネットワークを通じて外部に保存する場合】 医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。 (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、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。 (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	管理		C	106p，経産43p	

		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	（ク）	保存	2.バックアップルール ①総務省ガイドライン３．２．１ （２）（ウ４．①において実施するリスク分析結果に基づき情報システムの バックアップを取得する。バックアップの取得対象、取得頻度、保存方法 ・ 媒体、管理方法等を定め、その内容を運用管理規程等に含める。 ②①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、 記録内容の改ざん ・ 破壊等がないことを確認する。 ③記録媒体に格納するバックアップについては、その媒体の特性（テープディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。 ④③の対象となるバックアップの記録 媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。 ⑤①④の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う 。 ⑥バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 3冗長化措置 ①情報システム、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。 ②診療録等の情報をハードディスク等の記録機器に保存する場合、RAID 1又は RAID 6 相当以上のディスク障害対策を講じる。	管理		A	総務74p-	
保存性													
7.3	6.3		保存性					・保存性とは、記録された情報が法令等で定められた期間にわたって真正性を保ち、見読 可能にできる状態で保存されることをいう。 ・情報の損傷に対する備えを意味	管理		A	108p	
7.3			保存性		最低限 医療機関等に保存する場合	(1)	ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	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	管理		A	108p	

7.3			保存性		最低限 医療機関等に保存する場合	(2)	不適切な保管・取扱いによる情報の滅失、破壊の防止	1.　記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。 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容量（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.　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。 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	管理		B	109p	
7.3			保存性		推奨 医療機関等に保存する場合	(2)	不適切な保管・取扱いによる情報の滅失、破壊の防止	1.　記録媒体及び記録機器、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	管理		A	108p，経産43p	
7.3	6.3		保存性		最低限 医療機関等に保存する場合	(3)	記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	・記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごと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て、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又は記録機器については、そのデータを新しい記録媒体又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 ・耐用期間を超えないよう、また事業に支障を来	管理		B	109p	

7.3			保存性		推奨 医療機関等に保存する場合	(3)	記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	ハードディスク等の記録機器に保存する場合は、RAID-1 若しくはRAID-6 相当以上のディスク障害に対する対策を行う	管理		A	109p	
		3.2	安全管理に関する要求事項	3.2.3	技術的安全管理対策	（ク）	保存	1.保存管理 ①各医療機関等が利用可能な、保存可能資源の 残量については、随時提供できる措置を講じる。 ②医療機関等がサービスを利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、サービス仕様適合開示書 に基づき、医療機関等と合意する。 ③情報システムが情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量 、 保存可能期間、リスク等を運用管理規程等に含める。 ④③において、他の事業者が提供するクラウドサービスを利用する場合においても、同様の情報を収集して、対応する。仮想化技術による クラウド サービスを利用する場合には、クラウドサービス事業者が他の事業者との契約上利 用可能な資源に関する情報を確認する。 ⑤③により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。 ⑥サービスに係る委託先に対しても、③の運用管理規程に定める管理方法への対応等を求める。 4.毀損した情報の取扱い ①情報が毀損した場合、速やかに回復 する ための措置を講じ、その内容 ・ 手順等について、運用管理規程等に含める。 ②①に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。 ③②で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開	管理		A	総務74p-	
7.3			保存性		最低限 医療機関等に保存する場合	(4)	媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	1. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。 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。	管理		A	109p	

7.3			保存性		最低限 ネットワークを通じて外部に保存する場合	(1)	データ形式及び転送プロトコルのバージョン管理と継続性の確保	外部保存を受託する機関は、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	管理		A	109p	
7.3			保存性		最低限 ネットワークを通じて外部に保存する場合	(2)	ネットワークや外部保存を受託する機関の設備の劣化対策	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	管理		B	110p	
7.3			保存性		推奨 ネットワークを通じて外部に保存する場合	(1)	ネットワークや外部保存を受託する機関の設備の互換性を確保	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	管理		B	経産43p	
	6.3		保存性					法令等で定められた保存期間よりも長期の保存ができるよう事業継続に配慮	管理		C	111p	
8			診療録及び診療諸記録を外部保存する際の基準					対象文書は3.2参照	管理				
8			診療録及び診療諸記録を外部保存する際の基準	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						A	117p-	

8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	①	最低限	病院、診療所、医療法人等が適切に管理する場所に保存する場合 (ア) 病院や診療所の内部で診療録等を保存すること。 (イ) 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。 (ウ) 病院、診療所等であっても、保存を受託した診療録等について分析等を行う場合 は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。 (エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。 (オ) 情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、誤った閲覧が起こらないように配慮すること。 (カ) 情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されること。	管理		B	119p	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	推奨	(ア)	「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、プライバシーマークやISMS 認定等の第三者による認定を取得す	管理		A	118p	

8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	②	最低限	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若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) 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。 (ウ) 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。 (エ) 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、医療機関等は契約書等で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、情報漏えいや、誤った閲覧が起こらないようにさせること。	管理		A	115p	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	2	情報の取扱い		管理		B	119p	
			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	(イ)	推奨	「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」 ・プライバシーマークやISMS認定等の第三者による認定を受ける ・技術的な方法として、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 ・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、暗号化を行う、情報を分散保管する等。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。	管理		A	118p-	

8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	③	最低限	医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取扱いに対して監督を行えること。 (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」を遵守していること。 (ウ) 受託事業者が民間事業者等に課せられた経済産業省ガイドラインや総務省ガイドライン等を遵守すること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。 (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。なお保守に関しては、6.8を遵守すること。 (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。 (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、医療機関等は契約書等で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、情報漏えいや、誤った閲覧が起こらないようにさせること。	管理		B	119p	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.2	選定基準及び情報取扱基準	(ウ)	推奨	「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」 ・技術的な方法として、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 ・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、暗号化を行う、情報を分散保管する等。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。	管理		B	経産82p	
	8		診療録及び診療諸記録を外部保存する際の基準	8.1	選定基準及び情報取扱基準			厚労ガイドラインに従っていることを示せるよう、適用している安全管理策を適用宣言書の形で整理しておく	管理		A	経産121p	

		3.3	外部保存に関する要求事項	3.3.6	選定基準及び情報取扱基準			医療機関等に対する事業者情報の提供 サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。 ・医療情報等の安全管理に係る基本方針･取り扱い規程等の整備状況 ・医療情報等の安全管理に係る実施体制の整備 状況 ・実績等に基づく個人データ安全管理に関する信用度 ・財務諸表等に基づく経営の健全性 1.保守 ・ 運用における受託情報の閲覧制限 ①受託した医療情報を保守 ・ 運用を行うために閲覧 するのは必要最小限とする。 ②①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前 ・ 事後の 承認により実施する。 ③受託した医療情報を 緊急時に 閲覧した場合には、閲覧した受託情報の範囲及び 緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。 ④① における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また②③により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。 2.受託情報の閲覧制限のための機能 ① 予定された保守 ・ 運用等を行う際に受託 した医療情報 を許可なく閲覧できないようにするために、権限設定等の対策を講じる。 ② システム管理者、運用担当者、保守担当者等	管理		A	総務 144p-	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.3	個人情報保護	(1)	最低限	適切な委託先の監督を行う	管理		A	121p-	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.3	個人情報保護	(2)	最低限	・個人情報が特定の外部の施設に送られ保存されることについて、安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る。 ・患者から個人情報を収集する前に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 ・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行い、理解を得る ・患者本人に説明することが困難であるが、診療上の緊急性が特にない場合は、原則として親権者や保護者に説明し、理解を得る。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。	管理		C	123p	

		3.3	外部保存に関する要求事項	3.3.7	個人情報保護			①個人情報保護対応策を、 サービス仕様適合開示書に基づき、医療機関等と合意する。 ①医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書 に基づき、医療機関等と合意する。	管理		A	総務148p	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.4	責任の明確化			4,6.11参照	管理		C	123p	
8			診療録及び診療諸記録を外部保存する際の基準	8.1.5	留意事項			付則1参照	管理		C	123p	
8.2			電子媒体による外部保存を可搬媒体を用いて行う場合					付則1参照	管理		C	123p	
8.3			紙媒体のままの外部保存					付則2参照	管理		C	124p	
8.4			外部保存全般の留意事項	8.4.1	運用管理規程			6.3,4参照	管理		A	124p	
8.4			外部保存全般の留意事項	8.4.2	契約終了後の処理			・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、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査 ・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。 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 ・インデックスファイル、バックアップファイル	廃棄		A	124p	
8.4			外部保存全般の留意事項	8.4.2	契約終了後の処理			・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	廃棄		B	124p	
8.4			外部保存全般の留意事項	8.4.2	契約終了後の処理			・廃棄より前に、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	廃棄		A	経産83p	
	8		診療録及び診療諸記録を外部保存する際の基準	8.2	契約終了後の処理			・廃棄処理手順を定め医療機関等と合意 ・確実に廃棄されたことを医療機関等に保証 ・受領情報と管理情報の一覧の整合性を医療機関等が確認できるよう、預かっている情報について台帳を維持管理 ・台帳操作は特定の作業員だけが行い、複数人による確認等を行うことで、台帳上の情報の整合性について保証 ・再委託先でも同等の廃棄手段により確実に廃棄	廃棄		C	125p	

z		3.4	利用終了に関する要求事項	3.4.1	利用終了における対応			① サービスの一部又は全部の停止 やサービス変更の場合 （軽微なバージョンアップは含まない）には、サービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ② ① の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（ データ種類、期間等）、データ形式 データ項目、項目の詳細、ファイル形式）、返却方法、条件については、サービス仕様適合開示書に基づき、 医療機関等と合意する。また医療機関等のサービス利用 開始 後に、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。 ③ ② におけるデータの返却については、 厚生労働省ガイドライン第 5 版「5 情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合 があるので 、その旨も合わせて、 サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ ①においてサービスの 変更を含むサービスの一部 又は 全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等 で、②の対応は除く）、条件等について、 サービス仕様適合開示書 に基づき、医療機関等と合意する。 ⑤ 医療機関等の都合により 医療機関等のサービ	管理		A	総務151p	
8.4			外部保存全般の留意事項	8.4.3	保存義務のない診療録等			3.4参照	管理					
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					割愛	管理		A	133p, 付表1-3		
10			運用管理					運用管理規程は必ず定める。記載すべき内容は134p-。付表1-3が規程案（140p）。	管理		A	総務41p-		
		3.2	安全管理に関する要求事項	3.2.1	組織的安全管理対策	（ウ）	運用管理規程	厚労ガイドラインの9項目に沿って要求事項が示されている。	管理					
		3.2	安全管理に関する要求事項	3.2.7	情報・機器の持出	（ア）	運用管理規程等	機器・媒体の持出に関し運用管理規程等に定めるべき要求事項が示されている。	管理		A	総務101p-		
付則1			可搬媒体による外部保存					割愛	管理					
付則2			紙媒体による外部保存					割愛	管理					
		3.6	PHRサービス事業者における安全管理対策									総務154p-		

サービス仕様適合開示書等														
		4	安全管理の実施における医療機関等との合意形成の考え方	4.1	サービス仕様適合開示書による情報提供			・総務ガイドライン遵守を「サービス仕様適合開示書」を用いて示す。 ・医療機関は少ない負荷で総務ガイドラインへの適合状況を確認でき、クラウドサービス事業者と医療機関等とでサービス仕様適合開示書の内容を踏まえて契約する				総務 174p-	
				4.2	サービス仕様適合開示書によりされる内容情報提供			具体的な項目が示されている。				総務 176p-	
				4.3	契約、SLA等の文書による合意			・契約書のほか、SLAが策定され、合意文書を構成。SLAにはサービス仕様適合開示書で示されるサービス仕様やその前提条件などのほか、安全管理措置等に関する一般的な対応や、サービスレベル確保のための対応措置等、サービスレベルの評価等を含むことが想定される。				総務182p	
		別添	ガイドラインに基づくサービス仕様適合開示書・SLA参考例									総務 186p- （別添）	