『Reckoner』ガイドライン対応リファレンス

総務省版

2020 年 10 月 1 日

株式会社スリーシェイク

改訂履歴

版数	発行日	改訂内容
第 1 版	2020 年 10 月 1 日	初版発行

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
3.1 クラウドサービス事業者に対する要求事項の考え方			1	クラウドサービス事業者は、以下の要求事項に基づき、安全管理対策を行うとともに、医療機関等の管理者に対する十分な説明責任を実施。	当社サービスに係る情報処理の安全管理は、以下の経済産業省及び総務省によるガイドラインに準拠しており、その内容は本リファレンスにて開示する通りです。 ・経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」 ・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」当社は医療情報を受託管理するクラウドサービス事業者として、上記2省2ガイドラインの要求事項への対応を図っており、その内容は本リファレンスを含め、いつでも医療機関等の担当者が確認できるようにホームページ上に開示しています。これにより、医療機関等の担当者の方々が自院の運用管理規程を踏まえ、当社サービスをどのように利用・管理するかという観点より、手順書・管理規程の見直しを行えるようにしています。	適合可能
3.2.1 組織的安全管理対策	（ア） 組織・体制の整備についての要求事項	組織・体制の整備	2	サービスの提供についての管理責任を有する責任者の設置。	当社サービスの提供について、最終的な責任者である代表取締役ならびに事業責任者、システム責任者、個人情報管理責任者、サポート責任者を設置し、それぞれが連携を取りながらサービスの提供を行っております。	適合可能
			3	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）の設置。	当社サービスのシステム管理者については、技術的知識をもったうえでサービス提供における意思決定やインシデント対応での判断ができるようにしております。また、セキュリティ等専門性が問われる分野は、その専門に長けた管理者を配置しております。	適合可能
			4	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の設置。	情報システムの運用に関する事務を統括する責任者は、事業責任者として情報システム利用者の対応やインシデント対応を行っています。	適合可能
			5	No2～4に掲げた責任者の任命･解任等のルールを策定。	社内の人事ルールに基づいて、任命・変更を行うことができます。	適合可能
	（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	6	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。	当社サービスに係る守秘義務事項は、当社の契約条項のなかに守秘義務違反時のペナルティ項目を含め、定義しています。受託情報の取扱いに対する医療機関等による監督については、当社ホームページに掲載する本リファレンスにおいて、当社の取り組み状況を開示することで医療機関等が適切に監督・指示を行うための情報提供、及び必要に応じた対応を図るようにしています。	適合可能
		2.運用規定等の遵守	7	サービス提供に係る契約において、No10～15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。	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の遵守状況は本リファレンスに定める通りであり、契約に際しても本リファレンスに定める内容を遵守するものとなります。	適合可能
		3.関係ガイドラインの遵守	8	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。	当社サービスに係る情報処理の安全管理は、以下の経済産業省及び総務省によるガイドラインに準拠しており、その内容は本リファレンスにて開示する通りです。 ・経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」 ・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」 当社は医療情報を受託管理するクラウドサービス事業者として、上記2省2ガイドラインの要求事項への対応を図っており、その内容は本リファレンスを含めいつでも医療機関等の担当者が確認できるようにホームページ上に開示しています。これにより、医療機関等の担当者の方々が自院の運用管理規程を踏まえ、当社サービスをどのように利用・管理するかという観点より、手順書・管理規程の見直しを行えるようにしています。	適合可能
			9	No8に示す各ガイドラインの遵守状況を可能な限り具体的に医療機関等に提示。		適合可能
	（ウ） 運用管理規程についての要	1.基本方針と管理目的の表明	10	経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。	本サービスで扱う情報は、各クラウドデータベースやサービスへの接続情報のみのため、個人情報保護法の対象外となります。	対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
	求事項		11	No10の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。		対象外
			12	No10の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。		対象外
			13	情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定。	当社における情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーは本リファレンスに開示する通りの内容となります。	適合可能
			14	情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を実施。	当社では、システム責任者ならびに個人情報管理責任者監督のもと、各部署と連携をしながらリスク分析、ポリシー策定、対策実施、教育、監査をおこなう体制を構築しています。	適合可能
			15	情報セキュリティポリシーについて、サービス仕様適合開示書に基づく医療機関等との合意。	本リファレンスにて当社の情報セキュリティポリシーを開示することを通して、医療機関等にて当該内容が各機関で合意できる内容であるかを確認するための情報開示を行っています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
		2.サービス提供先の体制	16	サービスの提供に係る体制を、緊急時の対応も含めて明確にする。	当社ではGoogleが提供するクラウド基盤Google Cloud Platformにてサービス提供を行っているため、物理層の主管はGoogleとなることから、物理的なシステム環境が利用不可となる事態、あるいは悪意ある外部者によるプラットフォームを標的とするサイバー攻撃を想定した事業継続計画は独自では策定していません。当社所管の仮想層を対象とした、当社サービスの障害等の緊急対応プロセスには次の事項を含めて文書化及び関係者間の認識共有を図っており、当社の所管範囲で、サービス提供に影響のないようにしています。 ・障害発生時の全体フロー ・障害発生時の障害レベル判断手順 ・障害発生時の関係者の共有、対応人員の配置 ・一次対応手順 ・恒久対応手順 ・障害発生時の医療機関への周知フロー ・各所関係者への連絡フロー	適合可能
			17	サービスの提供に係る体制等に関する情報（再委託による体制に関する情報を含む）の開示等について、サービス仕様適合開示書に基づく医療機関等との合意。	当社サービスは、再委任を行なっておりません。当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	対象外
		3.契約書・マニュアル等の文書の管理	18	情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づく文書の管理。	本サービスで扱う情報は、各クラウドデータベースやサービスへの接続情報のみのため、個人情報保護法の対象外となります。 なお、下記の項目については、明文化するとともに、適宜見直しを行っております。 ・機器管理台帳 ・運用管理規定	適合可能
			19	サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理。		適合可能
			20	サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示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く医療機関等との合意。	当社サービスにおけるマニュアル等の文書管理は、資料のバージョン管理をしたうえで、管理者が最終確認の上、利用者に開示を行っています。サービス内容変更などにともない、随時文書は変更することがあります。	適合可能
			21	医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づく医療機関等との合意。	本サービスで扱う情報は、各クラウドデータベースやサービスへの接続情報のみを扱い、個人情報は扱わないため、本要件は対象外となります。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		4.リスクの発現の予防、発生時の対応の方法	22	サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。	本サービスで扱う情報は各クラウドデータベースやサービスへの接続情報のみのため、個人情報保護法の対象外となります。サービスに係る最大のリスクであるシステム障害については、No16の対応を図る体制としています。当社では、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。リスク分析表にて、保管・削除・破棄の観点で起こりうるリスクとそのリスク低減に対する管理策を記載しています。	適合可能
			23	サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		5.機器を用いる場合の機器等の管理	24	機器等の管理方法の文書化。	機器管理台帳にて記載し、記載内容は以下の通りです。 ・ハードウェア台帳 ・利用ソフトウェア台帳 ・ライセンス台帳 ・ライセンス証明書類	適合可能
			25	機器等について、台帳管理等により所在確認等を行う旨を定める。		適合可能
			26	機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		6.個人情報の記録媒体の管理方法	27	個人情報を記録した媒体の管理等に関する運用規程を策定。	本サービスで扱う情報は、各クラウドデータベースやサービスへの接続情報のみを扱い、個人情報は扱わないため、本要件は対象外となります。	対象外
			28	個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
		7.患者等への説明と同意を得る方法	29	医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づく医療機関等との合意。	当社サービスの提供範囲やクラウドサービス事業者が担う役割は、下記の通りです。 ・個人情報の扱いについて ・当社サービスの責任とその範囲 個人情報の扱いについては、本サービスでは、各クラウドデータベースやサービスへの接続情報のみを扱い、個人情報は扱わないため、本要件は該当しない認識です。 なお、当社では、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
		8.監査	30	サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等についての明文化。	運用管理規定に記載し、記載内容は以下の通りです。 ・サービスに供する機器や媒体の設置場所 ・万が一機器を紛失等した場合のプロセス ・ソフトウェア更新時（リリース時）のトラブル対応手順 ・ユーザに悪影響が発生し得る事象あった際の、更新の中止・延期を行い、対応した上での更新の手順 ・インシデント時の対応フロー ・情報セキュリティポリシーについては、リファレンス内に記載	適合可能
			31	第三者が提供するクラウドサービスを利用する場合について、これに対する監査又は代替する対応についての方針、内容の明確化。	当社ではGoogleが提供するクラウド基盤Google Cloud Platformにてサービス提供を行っています。Google Cloud Platformがどのように監査、または代替方法を実施しているかは、Googleのセキュリティに関するホワイトペーパー（https://cloud.google.com/security/overview/whitepaper?hl=ja、以下『Google Cloud Platform』対応セキュリティリファレンス）をご参照ください。	適合可能
			32	監査実施について記録し、当該記録の保存･管理方法の明確化。	情報システムに係る監査については実施しておりませんが、社内の機器管理、アクセス権の定期的な見直し、及びアクセスログ等のモニタリング等を行っています。	適合可能
			33	自社において実施する情報システム監査等について、サービス仕様適合開示書に基づく医療機関等との合意。	当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
			34	医療機関等に開示する監査記録等の範囲･条件等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		9.苦情・質問の受け付け窓口の設置	35	医療機関等の管理者からの問合せ窓口を設ける。受付の時間帯等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
			36	自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化。	当社ではGoogleが提供するクラウド基盤Google Cloud Platformにてサービス提供を行っていますが、当社サービスに関する問い合わせは全て当社にて対応しています。	適合可能
	（エ）運用管理規程に基づく文書類の整備についての要求事項	1.アクセス管理規程の策定	37	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。	当社では従業員による情報システムへのアクセス権限、アカウント管理、認証・パスワードポリシー、機器管理、定期的なIDパスワードの変更、アクセス権の定期的な見直し、従業員へのセキュリティ教育、情報システムのアクセスログ等のモニタリング等を行っています。サービスの提供に係るアクセスログのモニタリング等も行っており、その具体的な内容は本リファレンスをもって開示させて頂いています。	適合可能
			38	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。		適合可能
		2.委託契約に含めるべき事項	39	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な管理の実施。 ・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化。	本サービスで扱う情報は、各クラウドデータベースやサービスへの接続情報のみを扱い、個人情報は扱わないため、本項目は対象外となります。	対象外
3.2.2 物理的安全管理対策	（ア）サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項	1.施錠管理	40	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、施錠管理を実施。	当社サービスはGoogleが提供するクラウド基盤Google Cloud Platformに構築しているため、当該システムのサーバ・媒体等は外部事業者であるGoogleが運営するデータセンターで管理されています。詳細は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。当社サービスにリモートアクセスする端末については施錠管理を行っていませんが、当社パスワードポリシーに則ったログインパスワードを設定しているため、万が一、第三者に業務端末が渡っても、データへの不正アクセスは行えない対策としています。	適合可能
			41	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、施錠管理を実施。	当社サービスは、Googleが提供するクラウド基盤Google Cloud Platformに構築しているため、当該システムのサーバ・媒体等は外部事業者であるGoogleが運営するデータセンターで管理されています。詳細は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
			42	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、施錠管理を実施。		対象外
		2.アクセス制御	43	サービスに供する機器や媒体の設置場所について、許可された者のみが入退できるような制限。		対象外
			44	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）を定期的に実施。		対象外
			45	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、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。		対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			46	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、入退者の名札等の着用を義務化。		対象外
			47	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。		対象外
			48	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を見えないようにする。		対象外
			49	No43～48につき、運用管理規程等を規定。	当社は本リファレンスでアクセス制御の管理方針を開示することを通して、医療機関等で当該内容が合意できるものであるかを確認する体制としています。本リファレンスをご確認頂き、当社の管理体制についてご意見・ご要望がある場合は、個別のご相談とさせて頂きます。物理層に係る取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		3.サービスに供する機器や媒体を保存する施設	50	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。	本項目は当社の医療情報システムのクラウド基盤を提供し、物理的な機器や媒体を保存する施設を運営するGoogleの対応事項となるため、当社の対象外項目となります。Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
			51	No50の施設を設置する建築物において、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
		4.カメラによる監視	52	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。	当社サービスにリモートアクセスする端末を設置している当社の執務室については、スマートロックによる施錠管理を行なっており、許可された者のみ入室可能としております。物理層に係る取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			53	防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。		適合可能
			54	サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認できるようにする。		適合可能
	（イ）個人情報が参照可能な運用端末等に対する物理的安全管理対策としての要求事項	1.覗き見等の防止	55	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実施。	本サービスで扱う情報は各クラウドデータベースやサービスへの接続情報のみのため、個人情報は扱いませんが、当社従業員、外部事業者・派遣メンバについて、会社間ならびに該当する個人と守秘義務契約を締結しています。この守秘義務のなかで業務上把握した情報や業務秘密は就業中、及び退職後も一切口外しないことを求めており、外部へ漏洩しないようにする対策を講じています。覗き見の防止のため、運用端末に覗き見対策シートを貼り、運用者以外の視野に入らないよう対策をしております。	適合可能
			56	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実施。		適合可能
	（ウ）個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求	1.機器・媒体等の盗難・紛失防止	57	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実施。	本サービスで扱う情報は各クラウドデータベースやサービスへの接続情報のみを扱い、個人情報は扱わないため本要件は該当しない認識ですが、当社の保守運用作業においてもサーバのみにデータを管理することを可能とすることで、想定外のデータ保存が発生することのない仕組を整備しています。	適合可能
			58	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		適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
	事項			ーンの取り付け。		
			59	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を、自社の運用管理規程等に定める。		適合可能
3.2.3 技術的安全管理対策	（ア）利用者の識別及び認証に対する要求事項	1.利用者の識別	60	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を発行。（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は除く）	【当社サービスの仮想層に係る運用管理体制について】 当社が管理する仮想層の本番環境に係るアカウントは、担当ごとに全てユニークなアカウントを利用し、開発環境についてはGSuiteでアカウントをユニークに付与しています。当社が管理する仮想層の本番環境IDの使い回しやグループIDは使用しておらず、すべてユニークなIDで作業をしています。当社システムの本番環境での作業はすべてログを取得しており、どのアカウントでどういう操作をしたのかが把握できるようにしています。物理層における本取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。 【医療機関等におけるサービス利用者への提供機能】 当社サービスは、ユーザ毎に個別のアカウントを発行して利用する機能を提供しています。	適合可能
			61	利用者のなりすまし等を防止するための認証を実施。	【当社サービスの仮想層に係る運用管理体制について】 仮想層（当社管理）でID利用者なりすまし等を防止するため、パスワードによる本人認証を行っています。物理層における取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。 【医療機関等におけるサービス利用者への提供機能】 当社サービスではID利用者なりすまし等を防止するために、パスワードによる本人認証機能を提供しています。	適合可能
			62	利用者には医療機関等においてサービス利用する者の他、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。	本項目は利用者である医療機関の運用管理規程に係る内容のため、対応状況は略筆します。	適合可能
			63	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の発行は必要最小限とし、定期的な棚卸しを実施。	当社が管理する仮想層の本番環境IDの変更削除については、月に1度アカウントのクリーニング作業をしています。その時点で各ID保有者の利用状況や業務内容の変更有無、離職の有無を確認して、変更があるIDは変更削除を行っています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.本人識別のためにパスワードを設定する時のルール	64	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、それらを本人しか知り得ない状態に保つよう対策を実施。 ■具体例 ・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。	医療機関等が当社サービスの利用の際に設定可能なパスワードルールは下記のとおりです。 ＜技術的な対応＞ ・8文字以上 ・半角英数字を混在 ・記号を含める ＜運用面の対応＞ ・定期的にパスワードを変更するよう依頼 ・パスワードを複雑にするよう依頼 ・パスワードを使い回さないよう依頼	適合可能
			65	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	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の設定は行なっておりませんが、アクセスログの監視を行い、不正なアクセスを検知できる対応を実施しています。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				終わった場合の再入力に対して一定の不応時間を設定。 ・パスワード再入力の失敗が一定回数を超えた場合、再入力を一定期間受け付けない仕組み。		
			66	パスワードには十分な安全性を満たす有効期間を設定。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。	パスワードの有効期限を定めていないため、パスワードの世代管理は行なっておりません。	適合可能
			67	認証に際してID及びパスワードによらない場合でも、上記と同等以上の安全性の確保。	当社では運用管理面及び医療機関等へのサービス提供面双方において、ID・パスワードによる認証を採用するため、対象外となります。なお、物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		3.パスワードの管理	68	利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理。	利用者のパスワードは全てハッシュ化され保存されています。	適合可能
			69	サービスを提供する製品等の導入に際して、初期パスワードを変更するだけでなくアカウントの棚卸しを行い、不要なものについては削除を実施。	月に一度クリーニング作業を行っており、不要なアカウントを削除するようにしています。	適合可能
			70	利用者がIDやパスワードを失念した場合、予め策定した手順（本人確認を含む）に則り、本人へ通知又は再発行。	【当社サービスの仮想層に係る運用管理体制について】 当社が管理する仮想層の本番環境におけるパスワード再発行のフローは、管理者に連絡のうえパスワードをリセットの後に担当者が再度パスワードを再設定するフローを取っています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。 【医療機関等が当社サービス上で利用できる機能】 当社サービスのパスワード再発行は、医療機関の管理者権限をもった利用者が該当利用者のパスワードをリセットすることができます。そのため、利用者は管理者に問い合わせたうえ、パスワードをリセットしてもらった後に再度パスワードを再設定する手続きとなります。	適合可能
			71	パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知。	【当社サービスの仮想層に係る運用管理体制について】 仮想層の本番環境システムへのアクセスログ等、各種ログで不正や疑いがあったとき、またはパスワードが第三者に漏れた可能性がある場合は、該当するアカウントを停止し、その経由の原因調査ならびに再発防止策を行うプロセスをとっています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。 【医療機関等が当社サービス上で利用できる機能】 本事項は医療機関等でご対応頂く事項となります。	適合可能
			72	パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上でパスワードを無効化し、変更できるような対応を講じる。		適合可能
			73	利用者が設定するパスワードについて、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を実施。	医療機関等が当社サービス利用の際に設定可能なパスワードルールは下記のとおりです。 ＜技術的な対応＞ ・8文字以上 ・半角英数字を混在 ・記号を含める ＜運用面の対応＞ ・定期的にパスワードを変更するよう依頼 ・パスワードを複雑にするよう依頼 ・パスワードを使い回さないよう依頼	適合可能

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（平成３０年7月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			74	利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を実施。	パスワードの有効期限を定めていないため、パスワードの世代管理は行なっておりません。	適合可能
			75	利用者のパスワードポリシーについて、サービス仕様適合開示書に基づく医療機関等との合意。	上述した内容も含め、当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
		4.複数要素認証への対応	76	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で実施。	当社サービスの運用・開発業務におけるシステムへのログイン認証、及び医療機関等のユーザによるシステム利用時の認証方式はパスワードによる認証のみのため、2要素認証方式は特に採用していません。しかし、当社サービスにリモートアクセスする端末はログインパスワードを設定しており、端末を設置する執務室についても、警備会社の監視のもと施錠管理を行なっております。	適合可能
			77	利用者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く医療機関等との合意。		適合可能
			78	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、固定式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。		適合可能
			79	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、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。		適合可能
			80	代替的手段･手順を用いるケースにおいて、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。		適合可能
			81	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。		適合可能
			82	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く医療機関等との合意。		適合可能
	（イ）情報の区分管理とアクセス権限の管理に対する要求事項	1.情報管理区分	83	医療情報とそれ以外の情報を区分できる措置を講じる。	本サービスで扱う情報は各クラウドデータベースやサービスへの接続情報のみのため、医療情報は扱いません。	適合可能
			84	医療情報について、情報区分に従ってアクセス制御を行えるようにする。		適合可能
			85	仮想化技術を用いた資源をサービスに供する場合、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。	クラウド環境における仮想化技術を用いた資源管理はGoogleの管轄範囲のため、本事項への対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			86	医療機関等による情報資産の区分設定、これに対するアクセス制御の設定対応についてサービス仕様適合開示書に基づく医療機関等との合意。	当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
		2.権限設定	87	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。	職務権限に応じて情報操作が可能なメンバを管理することができます。当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			88	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。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く医療機関等との合意。		適合可能
			89	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。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く医療機関等との合意。		適合可能
		3.アクセス対象の設定	90	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。	当社サービスでは医療情報を扱わないため、患者毎に管理できる機能は提供しておりません。	対象外
	（ウ）ｅ-文書法の対象となる医療情報を含む文書等の作成における真正性の確保に対する要求事項	(a) 入力者及び確定者の識別及び認証に関する安全管理対策	91	ｅ-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く医療機関等との合意。 ・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。	当社サービスではｅ-文書法の対象となる医療情報を含む文書等を扱いません。	対象外
			92	ｅ-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く医療機関等との合意。 ・サービスとの連携におけるインタフェースの構築に関する役割分担。		対象外
		(b) 記録の確定手順の確立と、作成責任者の識別情報の記録に関する安全管理対策	93	ｅ-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く医療機関等との合意。 ・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。 ・確定記録の追記･削除の機能等に関する仕様。 ・確定記録の原状回復の機能等に関する仕様。 ・記録の自動確定機能等に関する仕様。 ・代替的な確定権限の機能等に関する仕様。		対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		(c) 更新履歴の保存に関する安全管理対策	94	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。	当社サービスは医療情報を扱っていないため本項目は対象外となります。	対象外
			95	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。		対象外
		(d)代行入力の承認機能に関する安全管理対策	96	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く医療機関等との合意。		対象外
			97	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。		対象外
			98	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)に関する機能を含める。		対象外
	（エ）アクセス記録(アクセスログ)に対する要求事項	1.アクセス記録の取得	99	情報システムへのアクセスを記録し、一定期間の保存。	アクセスログをクラウド（Google Cloud）上で9ヶ月保存しています。	適合可能
			100	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。	保存されるアクセスログには、ID、時刻、時間、そしてアクセス対象といった情報が含まれます。	適合可能
			101	アクセス記録の機能を有しない場合、サービス仕様適合開示書に基づく医療機関等との合意。	アクセス記録の機能はNo99,100の見解通りです。 No99,100の見解内容を含め、当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
			102	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。	当社サービスは、医療情報を一切扱わないため、本項目は対象外となります。	対象外
			103	No102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く医療機関等との合意。なお、本項におけるアクセス記録の管理方法についてサービス仕様適合開示書で保存期間を設けた場合、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。		対象外
			104	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。	本項目はサービス提供企業に求められる管理要件となりますが、No100に記載の通り当社サービスの運用管理業務において仮想層のアクセスログ、エラーログ、パフォーマンスログは常に監視しており、異常時には通知をトリガーに調査するような運用をしています。当社では本リファレンスをサービス仕様適合開示書の位置付けで医	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			105	No104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く医療機関等との合意。	療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.アクセス記録の保全のための要件	106	アクセス記録が保存されている資源に対してアクセス制限を行い、不正なアクセスを防止する。	【当社サービスの仮想層に係る運用管理体制について】 当社間の仮想層では下記の対策をしています。 ・ログ自体が改ざんされるリスクについて、ログデータは限られたシステム管理者しかアクセスできないようにしており、特権管理者以外は閲覧のみできる状態です。特権管理者のみが編集削除できるようにしており、担当者によるログ改ざんリスクを最小限にしています。 ・データ増加によりログが保存できなくなるリスクについて、ディスクの空き容量を監視し、定期メンテナンス時に必要に応じて容量を追加する運用をしています。 物理層における対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。 【医療機関等におけるサービス利用者への提供機能について】 当社サービスで提供している操作ログに関して、利用者は閲覧のみが許されており、編集等の改ざんはできないようになっています。直接ログを修正するにはログを保存しているデータベースを編集する必要がありますが、それは上記の運用管理態勢に記載ある対策を行うことで、改ざんが行われないよう対策をしています。	適合可能
			107	アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。		適合可能
			108	アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。		適合可能
		3.時刻の設定	109	アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で実施。	仮装層においてはGoogleが提供するGoogle Public NTPを使用しています。そのときのセキュリティ対策として各サーバのゲートウェイとなる入り口にファイアウォールを設置しており、外部からの通信は遮断するようにすることで当社サービスの開発運用上のアクセス記録、及び医療機関等の利用者によるアクセス記録の時刻の信頼性を担保するようにしています。よって、サービス利用者である医療機関等は当社サービス利用に際した時刻設定への懸念は当社にて対応させて頂いています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
	（オ） 端末等に表示される医療情報の漏洩に対する要求事項	1.端末表示からの漏洩対策	110	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。	当社サービスでは接続情報などは全て暗号化された状態で保存され、端末画面で暗号化されていない情報を表示することはありません。外部での作業時には覗き見防止用フィルターなどを設置する対策を講じています。	適合可能
			111	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な監視を実施。	当社サービスにリモートアクセスする端末を設置している当社の執務室はスマートロックによる施錠管理を行なっており、許可された者のみ入室可能としております。物理層に係る取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			112	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く医療機関等との合意。	No110,111の内容も含め、当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。物理層における本取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			113	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。	仮想層の本番環境のログインID（作業者ID）は、一定時間の未使用時には強制的にセッション遮断またはログオフする設定となっています。	適合可能
			114	医療機関等における利用者端末へのNo113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く医療機関等との合意。	当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
	（カ）情報漏洩対策等に対する要求事項	1.ウイルスやマルウェア等への対策	115	情報システムの構築に際して、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。	開発環境に用いる端末にはセキュリティソフトを導入しており、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）等の検知ができるようにしています。本番環境の仮想層は開発したプログラムと特定のライブラリ・サーバソフトしか導入しておらず、悪意のあるソフトウェア等の混入は開発環境で未然防止する体制のため、特にセキュリティソフト等の対策は行っておりませんが、常時本番環境上のログモニタリングを行うことで悪意のあるコードやソフトウェアの挙動有無を監視する取り組みを補完的に実施しています。物理サーバ層のセキュリティ対策はGoogleの主管範囲となります。そのため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			116	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。	開発環境におけるセキュリティソフトは当社管理者のみが設定を変更できるようにしており、インターネットに接続された時点で定義ファイル等は更新されるようになっています。本番環境における物理サーバ層に係る本項目の対応状況は、Googleの主管範囲となるため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			117	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を導入。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を適用。	開発環境におけるセキュリティソフトはネットワークに接続した段階で当社端末にインターネット経由で定義ファイルなどがアップデートされ、セキュリティソフトの設定でリアルタイムスキャン、定期的なファイルスキャン、外部記憶装置のスキャン、自動アップデートを行っております。OSのアップデートやパッチもネットワーク接続時にアップデートを行うようにしています。当社サービスの脆弱性について、脆弱性スキャナーツールでの巡回と定期的に第三者のセキュリティレビューを受けています。そこで発見された脆弱性については脆弱性の重要度・危険度に応じてレベル分けを行い、対応時期を決めた上で対応実施するように管理しています。本番環境における物理サーバ層に係る本項目の対応状況はGoogleの主管範囲となるため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			118	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、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。	当社サービスがウイルス等の攻撃で影響がでた場合、当社サービス内の通知サービスまたはメールにて医療機関の利用者に連絡します。サービス障害発生時（BCPで定義）同様のプロセスで対応を行っております。本番環境における物理サーバ層に係る本項目の対応状況はGoogleの主管範囲となるため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			119	情報システムの脆弱性に関する情報は、JPCERTコーディネーションセンター(JPCERT/CC)、内閣サイバーセキュリティセンター(NISC)、独立行政法人情報処理推進機構(IPA)等の情報源から、定期的及び必要なタイミングで取得して確認する。	脆弱性の情報収集は独立行政法人情報処理推進機構（IPA）を定期的に確認して、脆弱性があるソフトウェアの情報が掲載されている場合には、そのリスクを分析したうえで必要な対応策を講じています。本番環境における物理サーバ層に係る本項目の対応状況はGoogleの主管範囲となるため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.外部からの攻撃等への対策	120	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、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実施。	当社サービスでは医療情報を一切扱っておりません。本番環境に関するセキュリティゲートウェイは、当社サービスを構築・運用するクラウド基盤を提供するGoogleの主管となります。Googleによる本事項への対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。なお、Googleによるセキュリティ対策に加え、クラウド基盤上での当社サービス固有の取り組みとして、ファイアウォールによるポートや接続制限を行っています。	適合可能
			121	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	当社サービスでは医療情報を一切扱っておりません。当社の本番環境（仮想サーバ層）におけるネットワークセキュリティ対策は、ファイアウォールの設置以外はGoogleが主管しています。Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリ	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				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。	ティリファレンスをご参照ください。なお、Googleによる物理サーバ層のセキュリティ対策に加え、ファイアウォールによるポートや接続制限以外にクラウド基盤上での当社サービス固有の取り組みとして、仮想層にて以下を実施することで利用者が安全安心してサービスを利用できるようにしています。 ・ログ監視を通して異常検出をした際は、管理者にメールで通知が行われる仕組みの採用 ・異常検出した際は、原因分析・再発防止を検討した上で、システム上の対応を行うフローの整備本番環境における物理サーバ層に係る本項目の対応状況は、Googleの主管範囲となるため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	
			122	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実施。		適合可能
			123	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、個々の情報処理装置で同様の制御を実施。		適合可能
	（キ） 応答時間に関する要求事項		124	医療機関等がサービスを利用する際、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く医療機関等との合意。〞	システム導入前に試用期間を設けることで確認したものとしています。当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
	（ク） 医療情報等の保存に対する要求事項	1.保存管理	125	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、随時提供できる措置を講じる。	当社はGoogleから提供された情報をもとに、医療機関等へのサービス提供に影響が発生しないよう、資源確保等の対応を適宜行っています。医療機関等が当社サービスで利用可能なシステム資源の管理は、Googleのクラウド環境基盤Google Cloud Platformにて行われているため、本項目の対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			126	医療機関等がサービスを利用する際、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く医療機関等との合意。	医療機関等が当社サービスで利用可能なシステム資源に関する情報は、当社サービス資料に定義されています。また、本リファレンスをサービス仕様適合開示書の位置づけとしています。	適合可能
			127	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。	本サービスで扱う情報は各クラウドデータベースやサービスへの接続情報のみのであり、個人情報や医療情報は扱わないため、本項目は対象外となります。	対象外
			128	No127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、対応すること。仮想化技術によるクラウドサービスを利用する場合、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。		対象外
			129	No127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実施。	当社サービスの開発・運用に関与する従業員（外部パートナー企業からの派遣要員含む）には、Googleによる仮想化技術により割り当てられるシステム資源を用いてサービスが提供されていることについて就業前に教育を行っています。システム資源利用状況のモニタリング担当は専門的な知識を持つ運用管理の要員をアサインし、問題・課題を看過しないように周知徹底しています。	適合可能
			130	サービスに係る委託先に対しても、No127の運用管理規程に定める管理方法への対応等を求める。		適合可能
		2.バックアップルール	131	No22で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。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こと。	本項目は当社システムのクラウド基盤Google Cloud Platformを提供しているGoogleの対応事項となります。Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。当社においてもミドルウェアやアプリケーションにおける対策として、クラウド基盤上でデータの冗長化と定期的なバックアップを行っています。Googleのデータセンター災害時にも、医療機関等のデータを復元したうえで迅速に当社システムを復旧できる対策をしています。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			132	No131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行い、記録内容の改ざん・破壊等がないことの確認。	ミドルウェア、アプリケーション層におけるデータのバックアップは、Google Cloud Platform上に定期的にバックアップ保存しており、改ざん等の防止のために本データにはサーバ管理者のうち特権がある管理者のみアクセスできるようにしています。物理層に係る取り組み内容については『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			133	記録媒体に格納するバックアップについて、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。	当社サービスに係るバックアップデータはすべてGoogleが提供するクラウド基盤上にデータを世代別に複数保管する運用としているため、外部の記録媒体への保管は行っておりません。物理層に係る取り組み内容については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			134	No133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、終了日以前に別の媒体等にその内容を複写。		適合可能
			135	No131～134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実施。	バックアップに関する運用管理手順については、本業務を担当する従業員に周知のうえ、確実な運用を図るようにしています。物理層に係る取り組み内容については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			136	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く医療機関等との合意。	当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。上述の当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
		3冗長化措置	137	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。	本項目は当社のシステムのクラウド基盤Google Cloud Platformを提供しているGoogleの対応事項となるため、Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。当社においてもミドルウェアやアプリケーションにおける対策として、クラウド基盤上でデータの冗長化と定期的なバックアップを行っています。Google社のデータセンター災害時にも、医療機関等のデータを復元したうえで迅速に当社サービスを復旧できる対策をしています。	適合可能
			138	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。		適合可能
			139	No137を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づく医療機関等との合意。	事業継続計画を策定し運用することで問題発生時には適時に復旧できるようにしています。詳細は事業継続計画に記載しています。	適合可能
			140	障害時等に診療等が継続できる様にするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		4.毀損した情報の取扱い	141	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。	運用管理規定を策定し運用することで、情報が既存した際に速やかに回復するための措置を行える状態にしています。詳細は運用管理規定に記載しています。	適合可能
			142	No141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。		適合可能
			143	No142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示書に基づく医療機関等との合意。		適合可能
		5.保存データの見読性確保	144	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認。	本項目については医療情報を物理的に格納・保存するクラウド基盤Google Cloud Platformを提供しているGoogleによる主管事項となるため、『Google Cloud	対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			145	受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合(媒体の劣化、読取装置等のサポート切れ等)、速やかに代替的な措置を講じ、見読性確保の対応を実施。	Platform』対応セキュリティリファレンスをご参照ください。	対象外
	（ケ）ソフトウェア・機器等の品質管理に対する要求事項	1.情報システムに関するドキュメント作成	146	情報システムの機器及びソフトウェア構成図を作成。	当社サービスのソフトウェア構成、ネットワーク構成は属人的な管理とせず、社内の複数名の担当者で確認・レビューの上で文書として管理し、構成変更に応じて適時に更新を行っています。	適合可能
			147	情報システムのネットワーク構成図を作成。		適合可能
			148	No146,147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。	当社サービスを構成するシステムの構成については、Google Cloud Platformの管理画面から常に確認可能にしています。	適合可能
			149	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。	当社サービスを構成する機器やソフトウェア等の仕様及び更新履歴は、当社が利用しているプロジェクト管理ツールで一元的に管理しています。	適合可能
			150	No146～149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く開示内容、範囲、条件等を医療機関等と合意。	No146～149の内容は基本的に社内限の情報であり、一般に開示はしておりません。	適合可能
		2.品質管理に関する運用	151	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。	当社サービス（仮想層）に係る品質管理としては、ソフトウェアを更新（リリース）する際は事前に社内でテスト（結合テストならびに総合テスト）を行っており、更新時の思わぬ影響がでないように確認評価しています。更新するに当たり医療機関であるユーザに悪影響が発生し得る事象あった際は、更新の中止・延期を行い、対応した上での更新を行っています。上記の手順は適宜文書化した上で、従業員のスキルに依存しない品質管理を図るようにしています。なお、物理層における本取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			152	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実施。		適合可能
			153	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。	外部事業者・派遣メンバについても、機密情報保持規定の締結など、当社社員同様の業務教育を徹底しています。	適合可能
			154	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める。	不正な改ざんを防止する方法として、本番環境に更新するときは事前にテスト環境で動作テストならびにソースコードのレビューを行っています。意図しないプログラムがはいっていないか及び本番環境のリリース時は継続的インテグレーションツールで本番環境のリリースを自動化しており、手作業による操作ミスや特定の管理者以外が不適切なプログラムを入れることができないようにしています。脆弱性については社内セキュリティチームを設置し、プラットフォーム診断・ペネトレーションテストを定期実施し、脆弱性の管理を行なっています。上記の取り組みを通してシステム構成、ソフトウェアの動作状況の品質レビューを図っています。なお、物理層における本取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
	（コ）無線LAN・IoT機器の利用に対する要求事項	1.医療機関等における無線LANの利用	155	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や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く医療機関等との合意。	当社サービスはインターネット経由でサービスを提供する構成としており、医療機関等の内部におけるネットワーク構成は医療機関等の管理範囲となっています。	対象外
		2.IoT 機器を利用した	156	IoT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	当社サービスは医療機関等で運用されるIoT機器との接続を前提としないため、本項目は対象外となります。	対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		サービス提供時		ービス仕様適合開示書に基づく医療機関等との合意。		
			157	IoT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。		対象外
			158	IoT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。		対象外
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に関する対応	1.就業開始時における対応	159	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、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。	当社主管の仮想層におけるシステムの開発保守にかかわる従業員は、派遣社員や外部のパートナ企業の従業員も含め秘密保持契約を結んでいます。なお、物理層を管理するGoogleによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.就業時における教育等	160	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・訓練を実施。	当社サービスの開発保守にかかわる従業員はセキュリティ教育、セキュリティテストを実施しており、情報セキュリティの一定の知識と理解をもったうえで業務に取り組むようにしています。このテストは年に1回実施しており、定期的に教育しています。物理層を管理するGoogle Cloud Platform による取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			161	この教育・訓練を就業開始時及び就業後、定期的に実施。	No.160の教育・訓練は、就業開始時及び就業後に定期的に実施しています。	適合可能
		3.退職後の守秘義務等	162	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。	退社後の機密情報の管理は、秘密保持契約が退社後も有効になるようにしています。	適合可能
			163	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、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。		適合可能
			164	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、就業時における教育・訓練に含める。	当社サービスにかかわる従業員は、派遣社員や外部のパートナ企業の従業員も含め秘密保持契約を結んでいます。物理層を管理するGoogleによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		4.守秘義務違反者への対応措置	165	No159～164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。	当社は従業員ならびに派遣事業者と秘密保持契約を結んでいます。守秘義務に違反した場合は、発生した損害を賠償する義務があることを秘密保持契約内に記載しております。物理層を管理するGoogleによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		5.従業者等への教育状況・守秘義務等の状況	166	サービスの提供に従事する要員に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、サービス仕様適合開示書に基づく医療機関等との合意。	当社サービスに関する従業者等に対する守秘義務等に関する対応への取り組み状況は、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。なお、物理層を管理するGoogleによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
	（イ）再委託先に対する人的安全管理措置	1.委託契約に含めるべき事項	167	情報システム等に関する再委託を行う場合、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。	当社サービスは委託契約を行なっておりません。	対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			168	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。		対象外
			169	再委託に係る契約に、委託業務に係る守秘義務を含める。		対象外
			170	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認。		対象外
			171	再委託先が本ガイドラインに規定する安全管理対策を行っていることを確認。		対象外
3.2.5 情報の破棄に関する安全管理対策	（ア）情報の破棄に関する安全管理対策	1.情報の破棄の保証	172	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。	当社サービスは個人情報および医療情報は一切扱っておりません。電子情報記録媒体にコピーができないよう、アクセス制御を行っています。機密情報は全てインターネット上のクラウドツールを介して行っており、業務端末のローカルに保管しない業務運用としています。開発環境等で使用する端末のデータを破棄する場合、不可逆な抹消方式で破棄をしています。上記の通り、当社サービスに関する従業者等に対する情報の破棄の保証への取り組み状況は、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	対象外
			173	情報の破棄を実施した場合、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。		対象外
			174	No172で講じる措置及びNo173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く医療機関等との合意。		対象外
		2.情報破棄手順の文書化	175	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実施。 ・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)。		対象外
			176	情報の破棄手順について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
3.2.6 情報システムの改造と保守に関する安全管理対策	（ア）保守に用いるアカウント管理に関する安全管理対策	1.保守用のアカウント	177	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、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。	当社が管理する仮想層の本番環境および開発環境に係るアカウントは、担当ごとにGSuiteでアカウントをユニークに付与しています。	適合可能
			178	No177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て保存。	保存されるアクセスログには個人情報が特定できるIDが含まれています。	適合可能
		2.保守用アカウントの管理	179	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しないよう厳重に管理。	当社サービスの本番環境に影響がある作業は、一部の特権がある担当者のみが行うことができるようにしています。そのような作業をするときは、事前の承認プロセスで何をするのかを把握したうえで操作ログを取得しており、問題発生時に分析できるようにしています。	適合可能

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（平成３０年7月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
	（イ）保守実施に関する安全管理対策	1.リモートメンテナンス	180	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。	当社サービスはGoogleが提供するクラウド基盤Google Cloud Platformを用いてサービスを提供しているため、システムの開発・運用業務は全てリモートアクセス型となっています。この業務では、【（ア）保守に用いるアカウント管理に関する安全管理対策】に記載の通り、厳格な安全管理措置を講じています。なお、当社では、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
			181	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。		適合可能
			182	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く医療機関等との合意。		適合可能
		2.ログによる保守結果のレビュー	183	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て管理。		適合可能
			184	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。		適合可能
		3.医療機関等の施設内における保守対応	185	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く医療機関等との合意。	当社サービスの保守業務は医療機関等の施設内で行うことはありません。	対象外
		4.保守業務の実施報告	186	情報システムの保守業務を行う際、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実施。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く医療機関等との合意。	保守作業におけるダウンタイムは必要最低限となるよう事前に計画書を作成し、レビュー体制を構築することで品質管理をしています。保守作業に伴うリリース手順書について、レビュー体制を構築し品質管理をしています。システム停止を伴う作業の場合は、１週間前に事前に通知し承認を受けた上で実施します。	適合可能
			187	No186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、完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。		適合可能
			188	保守業務の実施にあたって、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。		適合可能
			189	No188に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づく医療機関等との合意。 本手順に基づき保守を行う際に必要となる事項等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
			190	No189で示された手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
			191	保守業務実施後には医療機関等に対し報告等を行い、医療機関等の管理者の確認を得		適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				る。本手順の対応について、サービス仕様適合開示書に基づく医療機関等との合意。		
	（ウ）保守に用いるデータの取扱いに関する安全管理対策	1.保守で用いるデータ	192	情報システムの動作確認に際して、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。	当社サービスの保守ならびにアプリケーション開発に用いるデータは受託医療機関のデータは利用しておらず、当社で作成したデータをもとに行っています。そのため、保守ならびにアプリケーション開発で利用する開発環境、テスト環境はそれぞれ当社で作成したデータを利用しています。当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
			193	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、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。		適合可能
			194	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、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		2.保守目的	195	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、その手順を策定。	当社サービスでは医療情報を一切扱いません。	対象外
			196	No195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く医療機関等との合意。		対象外
	（エ）保守における整合性・継続性確保のための安全管理対策	1.データ項目の標準形式の採用	197	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。	当社サービスでは診療録等のデータを一切扱いません。	対象外
			198	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、変換容易なデータ形式とし、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
		2.レコード管理方法等	199	医療情報に係るマスターテーブルの変更に際し、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。	当社サービスでは医療情報を一切扱いません。	対象外
			200	No199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く医療機関等との合意。		対象外
		3.データ形式及び転送プロトコルのバージョン管理と	201	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、サービスの利用に与える影響を確認。	当社サービスはクラウド型でWebブラウザを通じて利用するサービスのため、データ型式やプロトコルが変更するようなときは、事前にサーバ側でデータを変換ないし対応をした上でリリースをおこなっています。利用している医療機関はデータ形式やプロトコルの変更があった際も、そのことを意識することなくソフトウェアをシームレスに利用することができます。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		継続性の確保	202	No201の結果、サービスの利用に影響があると認められる場合、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実施。	サービスの利用に影響がある作業の場合、１週間前に事前に通知し承認を受けた上で実施します。	適合可能
			203	No202は他の情報システムとのデータ連携等を考慮して実施。医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づく医療機関等との合意。	当社サービスでデータ連携の仕様が変更になる場合、サービスに影響が出ないように変更をおこないます。連携しているサービスが終了する場合、当社サービス側の連携する機能を停止等の対応をユーザに実施していただきます。	適合可能
			204	データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、3.4に示す対策を講じる。		適合可能
		4.サービスに供する機器の劣化対策	205	サービスに供する情報システムに関する機器について、定期的に劣化状況に関する検査を行い、 必要な措置を講じる。	当社では開発・運用端末は定期的に買い替えするとともに、当該端末で用いるソフトウェアは常に最新化を図るようにしています。買い替えや最新化に際しては、サービス品質へ影響が発生しないように検証をおこなった上で導入を行っています。可搬式電子記録媒体にアクセス制御を行っているため、情報のコピーはできません。これらの取り組みを通して当社サービス環境上、機器の劣化によるサービス品質への影響を最小限化しています。この通り、当社サービスに供する機器の劣化対策への取り組み状況は、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
			206	サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合、サービスへの影響範囲について分析を行い、必要な措置を講じる。		適合可能
			207	サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合、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実施。		適合可能
			208	No207においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		5.サービスに供する情報システムの互換性確保や他の事業者のサービスとの関係	209	医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェアについて、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討。	当社サービスを構成する機器・ソフトウェア類については、当社の現行サービスへの影響を検証した上で常に最新化を図ることにより、互換性確保または標準仕様の変化への対応を図っています。	適合可能
			210	他のクラウドサービス事業者が提供するクラウドサービスを用いてサービスを提供する場合、他のクラウドサービス事業者がサービスを停止した際にも自社のサービス提供に支障が生じないように	当社サービスはGoogle Cloud Platformを用いてサービス提供しています。ただし、当社サービス内でデータを保持することはなく、仮にGoogle Cloud Platform自体のサービスの一部または全部の停止、大規模な変更が生じた場合においても、業務を継続するためのデータへのアクセスは実施することができます。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				するための対応策を検討し、対策を講じる。他のクラウドサービス事業者のクラウドサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更(軽微なバージョンアップは含まない)等が生じる場合、No206～208に示す対応策を講じる。		
			211	医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他クラウドサービス事業者のクラウドサービスの変更を行う場合、No209,210を考慮して実施。	ソフトウェアの構成を変更する場合、ないしはGoogleが提供するGoogle Cloud Platform以外のクラウドに変更する場合、事前に別の構成・環境での移行検証ならびに必要な改修を事前に行った上で、医療機関であるユーザに影響がでないように実施します。	適合可能
	（オ） 保守の体制・再委託に関する安全管理対策	1.保守体制の変更	212	情報システムの保守等の体制変更が生じた場合、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く医療機関等との合意。	当社サービスはGoogleが提供するクラウド基盤Google Cloud Platformを用いてサービスを提供しており、その保守・運用は様々な手順・マニュアル類に文書化することで、特定の担当者へナレッジが依存しないようにしています。こ保守・運用体制の変更が仮に発生しようとも、医療機関等の医療機関等への影響を極小化する体制としています。上述の内容も含め、当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。上述の当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。なお、物理層を管理するGoogleによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.再委託先の体制	213	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、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。	当社サービスは保守業務を委託していないため、本項目は対象外となります。	対象外
			214	No213の実施状況に関して、契約実施ごと又は定期的に外部事業者に対して報告を求めて確認。		対象外
3.2.7 情報及び情報機器の持ち出しについての安全管理対策	（ア） 運用管理規程等に関する安全管理対策	1.機器・媒体の持ち出しに関する方針策定	215	サービスに関する情報(受託情報、情報システムに関連する情報等)を格納する機器・媒体等の持ち出し(委託元からの持ち出しを含む)に関する方針及び規則等を、運用管理規程に定める。		対象外
			216	No215における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含める。		対象外
			217	No216で定める内容について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
		2.サービスに供する記録媒体・記録機器に関する対応	218	サービスに供する記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体・記録機器の取扱い ・サービスに関する情報(受託情報、情報システムに関連する情報等)を格納する機	当社サービスでは情報記録電子媒体にコピーできないようにアクセス制御がされています。私的端末の業務利用（Bring Your Own Device）は原則禁止しており、可搬型電子媒体や私的端末等に情報を保管し、持ち出しを行おうとする不正な行為に対して、監視カメラ等による監視を行っています。従業員及び業務委託について、採用時に機密保持契約を締結しています。仮にインターネットを介して情報の持ち出しが行われた場合、どの情報にいつだれがアクセスしたかを監視・追跡できる対策を施	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				器・媒体等の持ち出し(委託元からの持ち出し含む)に関する方針及び規則等(「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含める。) ・サービスに関する情報を持ち出した場合、当該情報を格納する機器・媒体等の盗難・紛失(持ち出し時の機器・媒体等の物理的な盗難、紛失)のほか、システム管理者が承認しない外部への送信等(第三者による悪意の送信、従業者等における誤送信等を含む。)が起きた場合の対応 ・外部のネットワークに接続する場合の接続条件、安全管理措置等(格納された情報の漏洩や改ざんが生じないようにするための具体的な措置、マルウェア対策、ファイアウォール導入等)	しています。物理層を管理する Google Cloud Platform による取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	
		3.従業員等及び委託先に対する対応	219	No218に示した内容に関する教育を従業員等に対して実施。		適合可能
			220	上記の運用管理規程について、再委託先に対しても遵守等を求める。		適合可能
		4.医療機関等との合意	221	No218～220に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づく医療機関等との合意。	上記の通り「サービスに供する記録媒体･記録機器に関する対応」「従業員等及び委託先に対する対応」「医療機関等との合意」についての取り組み状況は、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。	適合可能
	（イ） 機器・媒体の台帳管理		222	サービスに関する情報を格納する機器･媒体等について、台帳管理等を行い、定期的に所在確認。	当社サービスでは個人情報および医療情報を一切保存しません。	適合可能
	（ウ） 情報機器等の持ち出しにおける漏洩対策に関する安全管理対策	1.起動パスワードの設定	223	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実施。	サービス提供に直接的に関係する物理的サーバ・機器はGoogleの主管範囲のため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。当社内部で使用する業務端末については、特に起動時のパスワード（BIOSパスワード）は設定していませんが、ログインパスワードの設定を行っているため、万が一第三者に業務端末が渡っても、データへの不正アクセスは行えない対策としています。	適合可能
			224	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。	サービス提供に直接的に関係する物理的サーバ・機器はGoogleの主管範囲のため『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。なお、当社内部で使用する業務端末については、当社パスワードポリシーに則ったパスワードを設定しています。当社パスワードポリシーは以下です。 ＜技術的な対応＞ ・半角英数字混在 ・大文字小文字の両方を使用 ・記号を使用 ・8文字以上 ＜運用面の対応＞ 業務端末利用者に以下の周知を徹底しています。 ・定期的なパスワードの変更 ・パスワード使い回し禁止 ・類推困難な複雑なパスワードの設定	適合可能
			225	サービスに関する情報を格納する情報機器のログイン及びアクセスについて、複数の認	当社サービスでは個人情報および医療情報を一切保存しないため、パスワードの設定のみを行っております。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				証要素を組み合わせて実施。		
		2.機器を持ち出す場合の手順	226	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、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、パスワード設定する等の事項を含める。	当社サービスでは個人情報および医療情報を一切保存しません。クラウド上の情報は操作PC及び外部記録媒体にコピーできないようにアクセス制御がされています。	適合可能
		3.持ち出し機器等におけるアプリケーション	227	サービスに関する情報を格納する機器を持ち出す場合、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。	持ち出しをする可能性がある業務端末については、業務に必要なソフトウェアのみを使うことをルールとして周知しています。必要なソフトウェアがある場合、検証端末を利用するように周知・運用しています。	適合可能
			228	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。	業務端末へのアプリケーション追加インストールの技術的な制限は行っていませんが、不必要なアプリケーションをインストールしないように利用者に周知を図っています。持ち出しの有無を問わず業務端末には、セキュリティ対策ソフトを導入しており、ウイルス等の悪意あるプログラムに対する対策を講じています。	適合可能
		4.BYOD への対応	229	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。	当社では私的端末の業務利用（Bring Your Own Device：BYOD）は原則禁じています。	適合可能
			230	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、サービス仕様適合開示書に基づく医療機関等との合意。具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏えい等を防止する観点から、例えば仮想デスクトップを用いてOSレベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。		適合可能
		5.公衆無線 LAN の利用禁止	231	業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合、公衆無線LANへの接続は行わない。	当社では業務端末を社外で利用する場合、必ず暗号化されたネットワークを利用し、オープンネットワークには接続しないルールを策定しており、当該ルールに基づく社内教育をおこなっています。	適合可能
3.2.8 災害等の非常時の対応についての安全管理対策	（ア）障害時における見読性確保に関する安全管理対策	1.障害時の責任分界	232	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く医療機関等との合意。	物理ネットワーク・物理機器、ミドルウェアについてはGoogleが提供するGoogle Cloud Platformが管理主体としています。仮想層、仮想ネットワーク、アプリケーションの管理主体は当社の責任になります。当社サービスにアクセスするまでのネットワークのうちインターネットサービスプロバイダーが主管しているものはユーザが管理主体としています。障害発生時の責任分界は、上述の内容も含め本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。上述の当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。物理層を管理するGoogle Cloud Platformによる取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		2.医療機関への情報提供	233	医療情報を医療機関等に保存する場合、障害時における見読性確保のために医療機関等	当社サービスでは個人情報および医療情報を一切保存しません。実際のデータはユーザが管理している接続情報で閲覧できます。本リファレンスをサービス仕様適合開	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				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く医療機関等との合意。	示書の位置付けで医療機関等に開示しています。	
		3.外部ファイル等の出力	234	医療情報を医療機関等に保存する場合、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く医療機関等との合意。		適合可能
		4.遠隔地のバックアップに関する見読性	235	医療情報を医療機関等に保存する場合、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く医療機関等との合意。		適合可能
		5.見読性の確保の支援機能	236	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づく医療機関等との合意。		適合可能
	（イ）災害等の非常時の対応に関する安全管理対策	1.BCP 等の策定	237	サービスに係るBCP及びコンテンジェンシープランを策定。	事業継続計画を策定し運用することで問題発生時には適時に復旧できるようにしています。詳細は事業継続計画に記載しています。	適合可能
			238	No237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。		適合可能
			239	No237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く医療機関等との合意。		適合可能
		2.非常時のサービスの運用	240	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く医療機関等との合意。	実際のデータはユーザが管理している接続情報で操作可能なため、非常時使用のアカウントは提供しておりません。	適合可能
			241	非常時に用いる利用者アカウントの利用状況を定期的にレビュー。		適合可能
			242	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。		適合可能
			243	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、正常復帰後に速やかな無効化を図る。		適合可能
		3.サイバー攻撃等への対応	244	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、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。	当社所管の仮想層のアクセスログ、エラーログ、パフォーマンスログは常に監視しており、システム障害あるいは外部攻撃の発生に伴う異常時には通知をトリガーに調査するような運用をしています。物理層を管理するGoogle Cloud Platformによる取り組み状況は『Google	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
					Cloud Platform』対応セキュリティリファレンスをご参照ください。	
			245	No244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実施。	サービスに障害が発生した場合、開発責任者の承認の元でユーザに状況及び復旧の見通しについて報告します。	適合可能
			246	No244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く医療機関との合意。	システム障害あるいは外部攻撃の発生に伴う異常時には、状況及び復旧の見通しといった内容をテキストデータで報告します。	適合可能
			247	No246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。	当社サービスはGoogle Cloud Platformの東京リージョンを基盤として提供しています。	適合可能
		4.サービス回復後のデータ整合性の確保	248	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・検証方法の規定等)を講じる。	当社サービスは医療機関等から預託された情報を扱いません。	適合可能
3.2.9 個人情報を含む医療情報を外部と交換する場合の 安全管理対策	（ア） ネットワークに関する安全管理対策	1.ネットワーク経路における全般的な安全管理対策	249	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)を実施。	本番環境に関するセキュリティゲートウェイは、当社サービスを構築・運用するクラウド基盤を提供するGoogleの主管となります。Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。Googleによるセキュリティ対策に加え、クラウド基盤上での当社サービス固有の取り組みとしてファイアウォールによるポートや接続制限を行っています。ログ監視を通して異常検出をした際は、管理者にメールで通知が行われる仕組みを採用しています。異常検出した際は原因分析、再発防止を検討した上で、システム上の対応を行うフローの整備をしています。医療機関等が当社サービスにアクセスする際は、TLS1.2での接続及びクライアント証明書を必須にしており、クライアント証明書が認証された端末からのみアクセス可能としています。	適合可能
			250	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)を実施。	当社サービスはサーバ側でのTLS1.2のサーバ証明書、ならびにTLS1.2のクライアント証明書の両方式を採用することで、アクセス先のなりすまし等の対策を講じています。	適合可能
			251	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く医療機関等との合意。	当社はインターネットを介したサービス提供を行っているため、ネットワーク経路の安全措置はNo249,250で記載する方針に基づき行っており、閉域ネットワーク等を用いたサービス提供は実施していません。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ついては、物理層を管理するGoogleによるセキュリティ対応策を前提とした観点より、医療機関等への安全かつ継続的なサービス提供を可能とする追加措置として、No249,250に記載する当社の仮想層の取り組みを行っています。上述の内容も含め、当社では本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。上述の当社の管理体制について追加的なご要望がある場合は、個別のご相談とさせて頂いています。当社の取り組みの前提となるGoogleによる対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			252	ネットワーク経路の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く医療機関等との合意。		適合可能
			253	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		適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				に関する情報について、サービス仕様適合開示書に基づく医療機関等との合意。		
		2.医療機関等からのネットワーク経路の確認	254	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実施。	当社サービスに対して医療機関等がアクセスするまでに必要となる施設内部の物理的なネットワーク、及びISP事業者が提供するインターネットサービスは、医療機関等の医療機関等の主管範囲とさせて頂いています。 よって、本事項は当社の管轄範囲外となります。	対象外
			255	No254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互認証を実施。	当社サービスは他のクラウドサービス事業者とのサーバ間接続はおこなっていないため、本項目は対象外となります。	対象外
			256	No254において、事業者が保守業務を再委託している場合、事業者と再委託先との接続では、別途なりすましを防止する策を講じる。	当社サービスに対して医療機関等がアクセスするまでの施設内部の物理的なネットワーク、及びISP事業者が提供するインターネットサービス自体は、医療機関等の医療機関等に決定・管理頂くもので、医療機関等の主管範囲とさせて頂いているため、本事項は当社の管轄範囲外となります。	対象外
			257	厚生労働省ガイドライン第5版6.11C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
		3.ネットワーク経路対応に用いる機器	258	ルータ等のネットワーク機器は、ISO15408が規定するセキュリティターゲット又はそれに類する文書が本ガイドラインに適合しているものを選定。	当社サービスはGoogleが提供するクラウド基盤Google Cloud Platform上で提供されているため、医療機関等から当社サービスにインターネットを経由してネットワーク接続する際に必要となる物理的なネットワーク機器類の主管はGoogleとなります。よって、本事項は当社の管轄範囲外となります。Google Cloud Platformの対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			259	ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関するクラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
		4.暗号化対策	260	送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施。	データ送受信の際の安全性については、通信をTLS1.2でクライアント証明書を入れることで暗号化しており、改ざんや傍受防止をしています。	適合可能
			261	サービスの提供においてSSL/TLSを用いる際、TLS1.2に対応した措置を講じる。		適合可能
			262	No261のほか、医療機関等がメール暗号化(S/MIME等)やファイル暗号化への対応を求める場合、対応に必要な措置及び条件等について、サービス仕様適合開示書に基づく医療機関等との合意。	サービス導入前に当社サービスの仕様をご説明させていただき、トライアル期間も含めて問題ないことを確認いただいた上で契約締結しています。本リファレンスをサービス仕様適合開示書の位置づけとしています。	適合可能
		5.通信経路の暗号化対策	263	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、TLS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の高い「高セキュリティ型」に準じた適切な設定を実施。	当社サービスはオープンネットワークを利用しますが、サーバ証明書・クライアント証明書ともにIPAが推奨するSSL/TLS暗号設定ガイドラインの高セキュリティの各項目（TLS1.2、鍵長等）を充足した体制でサービスを提供しています。物理層に係るGoogle Cloud Platformの対応状況は『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	適合可能
			264	SSL-VPNは、原則として使用しない。	当社サービスではSSL-VPNは利用していません。物理層に係るGoogle Cloud Platformの対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
					照ください。	
			265	サービス提供に際してソフトウェア型のIPsec又は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)等による攻撃について、適切な対策を実施。	当社サービスの提供側のネットワークはオープンネットワークとの接続口にゲートウェイを設定しており、不必要な通信やアクセスがないようセキュリティ対策をしています。物理層に係るGoogle Cloud Platformの対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			266	医療機関等における利用者がソフトウェア型のIPsec又は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)等による攻撃についての適切な対策に関する情報を提供。情報提供の範囲、条件等について、サービス仕様適合開示書に基づく医療機関等との合意。	医療機関等に当社サービスを利用する端末にセキュリティ対策ソフトを導入頂くことで、オープンネットワークに接続している端末がマルウェア等のサイバー攻撃を受けることによるTLS1.2のセッション間の回り込みリスクを低減する対策としています。物理層に係るGoogle Cloud Platformの対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		6.回線の品質等	267	回線の管理、品質等に対す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く医療機関等との合意。	当社サービスに対して医療機関等がインターネットを経由してアクセスするネットワークは、医療機関等の医療機関等の責任範囲とさせて頂いているため、本事項は当社の管轄範囲外となります。当社サービスはGoogleが提供するクラウド基盤Google Cloud Platform上で提供されているため、医療機関等から当社サービスへのネットワーク接続に際して用いられる物理的なネットワーク機器類の主管はGoogleとなります。なお、Google Cloud Platformの対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		7.医療機関等の外部からのサービス利用	268	医療機関等の利用者が医療機関等の外部からサービス利用する場合、医療機関等の利用者が用いるPC作業環境に仮想デスクトップ等の技術を導入する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く医療機関等との合意。	当社サービスはWebブラウザ経由で利用するため、利用者が用いるPCについては特に指定なしでご利用いただけます。	適合可能
	（イ）保守における通信上の安全管理対策		269	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。	当社サービスはGoogle提供のクラウド基盤Google Cloud Platformを用いてサービスを提供しているため、システムの開発・運用業務は全てリモートアクセス型となっています。業務における安全管理措置は、【3.2.6情報システムの改造と保守に関する安全管理対策-（イ）保守実施に関する安全管理対策】に記載の通りとなります。	適合可能
	（ウ）医療機関等との責任分界に関する取り決め	1.通信経路に関する責任分界	270	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6.11C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く医療機関等との合意。	当社がサービス提供でネットワーク通信にて担う役割・責任範囲は、Google管理のクラウド基盤Google Cloud Platformの上に構築した仮想的なネットワークの範囲のみとなります。本ネットワーク範囲についてアクセスログ、エラーログ、パフォーマンスログは常に監視しており、異常時には通知をトリガーに調査する運用を行っています。医療機関等がインターネットを経由して当社サービスへアクセスするまでのネットワーク範囲は、医療機関等の医療機関等の責任範囲とさせて頂いているため、本事項は当社の管轄範囲外となります。医療機関等から当社サービスへのネットワーク接続に際しては、Google主管の物理的なネットワーク機器類との接続が行われていますが、当該機器についてはGoogleの主管範囲となっています。Google Cloud Platformの取り組み状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
			271	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く医	医療機関等が当社サービスとデータの送受信をインターネット経由で行う場合、通信経路を全てTLS1.2で暗号化しており、医療機関等/当社サービス間で送受信データの機密度が低下しないようにしています。	適合可能

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				療機関等との合意。		
			272	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く医療機関等との合意。	当社サービスに関する通信経路に関する責任分界については、本リファレンスの開示をもって医療機関等へ情報提供を行う体制としています。当社の管理状況についてご意見・ご要望がある場合は、個別のご相談とさせて頂いています。	適合可能
		2.患者等が閲覧する場合の手続・責任分界	273	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、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く医療機関等との合意。	当社サービスは医療情報を一切扱っていないため、本項目は対象外となります。	適合可能
			274	医療情報を患者等の閲覧に供する場合、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く医療機関等との合意。		適合可能
			275	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く医療機関等との合意。		適合可能
3.2.10 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の安全管理対策	（ア）電子証明書による電子署名		276	法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、保健医療福祉分野PKI認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。	当社サービスは保健医療福祉分野PKI、ならびにこれに類する電子署名機能を提供していません。	適合可能
			277	保健医療福祉分野PKI認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名・押印を電子署名で行うサービスを提供する場合、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づく医療機関等との合意。電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律(平成12年法律第102号)」第2条1項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には上記要件を担保できることを示して、当該サービスに		適合可能

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（平成３０年7月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
				おける本人確認方法及び検証方法について、サービス仕様適合開示書に基づく医療機関等との合意。		
			278	公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
	（イ） タイムスタンプの付与		279	電子署名を施す情報に対してタイムスタンプを付与。この場合、タイムスタンプの内容・検証方法について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
			280	タイムスタンプを付与した情報を取り扱う場合、法定保存年限内における当該タイムスタンプ有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
			281	タイムスタンプを付与した情報を取り扱う場合、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
	（ウ） タイムスタンプを付与する時点で有効な電子証明書の使用		282	タイムスタンプを付与した情報を取り扱う場合、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づく医療機関等との合意。		適合可能
3.3.6 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準	（ア） 医療機関等によるサービス選択のための事業者情報の提供		283	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、以下の情報を提供。 ・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〞	当社サービスは医療情報および個人情報を扱っておりませんが、これまでデータの流出及び不当利用などが行われていない実績があります。現在ISMSの取得を目指しており、これまで以上にデータの安全管理体制を強化するべく取り組んでおります。取扱規定等の整備状況につきましては、本リファレンスの開示をもって医療機関等へ情報提供を行う体制としています。	適合可能
	（イ） 受託情報に対する閲覧制限	1.保守・運用における受託情報の閲覧制限	284	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。	当社サービスは医療情報を一切扱わないため、本項目は対象外となります。	対象外
			285	N284の閲覧が必要な場合、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。		対象外
			286	受託した医療情報を緊急時に閲覧した場合、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。		対象外

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（平成３０年７月）					対応状況	
項目番号			No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			287	No284～286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く医療機関等との合意。 No285,286により医療情報を閲覧した場合、速やかに医療機関等にその旨を報告。		対象外
		2.受託情報の閲覧制限のための機能	288	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。		対象外
			289	システム管理者、運用担当者、保守担当者等が意図しない閲覧を行わないことを担保するための措置(データベースの暗号化等)を講じる。		対象外
	（ウ） 受託情報の解析及び第三者提供制限	1.受託情報の解析等の制限等	290	受託した医療情報の解析・分析は、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。		対象外
			291	受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。		対象外
		2.受託情報の解析等の第三者提供制限	292	受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。		対象外
			293	No292の内容を、サービス提供に係る契約に含める。		対象外
			294	医療機関等の指示に基づき受託した医療情報の第三者提供(閲覧)を行う場合、医療機関等が許諾した者以外が閲覧・取得できないように、3.2.3及び3.2.9に示す対応策を講じる。		対象外
			295	No294により第三者提供(閲覧)を行う場合、閲覧・取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者(医療情報連携ネットワーク等)の指示に基づき、速やかに変更・削除できる対応を実施。		対象外
			296	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合、医療機関等に対してその内容(提供先(閲覧者)、閲覧情報、閲覧日時等)を報告。		対象外
			297	No292～296により第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外
3.3.7 個人情報の保護についての安全管理対策	（ア） 診療録等の外部保存委託先の事業者内における個人情報保護		298	個人情報保護対応策について、サービス仕様適合開示書に基づく医療機関等との合意。	当社サービスは個人情報を一切扱わないため、本項目は対象外となります。	対象外
	（イ） 外部保存実施に関する患者への説明		299	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		対象外

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（平成３０年７月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			ついて、サービス仕様適合開示書に基づく医療機関等との合意。		
3.4.1 クラウドサービスの利用終了における対応		300	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)、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実施。	保守作業におけるダウンタイムは必要最低限となるよう事前に計画書を作成し、レビュー体制を構築することで品質管理をしています。システム停止を伴う作業の場合は、１週間前に事前に通知し承認を受けた上で実施します。	対象外
		301	No300の場合、受託した医療情報を医療機関等に返却。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く医療機関等との合意。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、No300に準じた対応策を講じる。	当社サービスは医療情報を一切扱わないため、本項目は対象外とします。	対象外
		302	No301におけるデータの返却について、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の合意。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く医療機関等との合意。	当社サービスはデータの保管を行わないため、データの返却はせず接続情報の破棄を行います。本リファレンスをサービス仕様適合開示書の位置づけとしています。	適合可能
		303	No300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、No315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く医療機関等との合意。	本リファレンスをもって合意されたものとしています。	適合可能
		304	医療機関等の都合により医療機関等のサービス利用が終了する場合も、No301,302に示す対応策を講じる。	当社サービスはデータの保管を行わないため、接続情報のみ削除する対応を取らせていただいています。本リファレンスをサービス仕様適合開示書の位置づけとしています。	適合可能
		305	サービス提供の停止又は医療機関等におけるサービス利用停止が生じた場合、速やかに記録の削除、媒体の廃棄等を実施。記録の削除、媒体の廃棄等を行った場合、これを証明する資料を医療機関等に対して提出。		適合可能
		306	No305に関して、医療機関等へのサポート(所管官庁への情報提供含む)等に関連して必要最低限の範囲で記録を保	医療機関等のユーザが当社サービスの利用終了後において一部のデータ等をサービス上に残したいと希望した場合、データはサーバ上に継続して保管し、データの管理方法、安全管理措置等については利用している医療機関	適合可能

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（平成３０年７月）			対応状況	
項目番号	No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		持し続ける場合、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づく医療機関等との合意。	同様の内容でおこないます。サービス終了後もデータを保持する場合の取り組み状況は、本リファレンスをサービス仕様適合開示書の位置付けで医療機関等に開示しています。当社の運用管理状況についてご意見・ご要望がある場合は、個別のご相談とさせて頂いています。	
	307	No300～306についての手順等を、運用管理規程等に含める。	当社サービスに関するクラウドサービスの利用終了における対応方針については、本リファレンスをサービス仕様適合開示所として開示することをもって医療機関等へ情報提供を行うこととしています。当社の管理方針についてご意見・ご要望、または医療機関等にて患者等への説明に際して追加的な情報提供が必要となる場合、個別のご相談とさせて頂いています。	適合可能
3.5.2 オンライン診療システム提供事業者における要求事項	308	オンライン診療システムにおいて、医療情報システムとの接続がある場合、本チェックリスト3.2～3.4を適用し確認。	当社サービスはオンライン診療システムには該当しないため、本項目は対象外となります。	対象外
	309	患者側端末で利用するオンライン診療システムの機能には、オンライン診療の実施中に医療情報システムと接続する機能等を含まない、及びこれ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く医療機関等との合意。		対象外
	310	医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づく医療機関等との合意。		対象外