医療情報システム向け
使えるクラウドバックアップ
利用リファレンス

(総務省版)

2019年12月2日版

使えるねっと株式会社

長野本社：〒380-0836 長野県長野市南県町1082 KOYO南県町ビル3階

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
1	3 クラウドサービス事業者に対する安全管理に関する要求事項	3．2 医療情報サービスに求められる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・体制の整備についての要求事項	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。	弊社の使えるクラウドバックアップは、サービス提供を管理するために十分な技術能力および経験を保有する責任者（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）を設置しており、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。
2						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。	同上
3						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。	同上
4						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。	弊社では、責任者の任命・解任等について、弊社内の人事ルールに基づいて行っております。
5				(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。	弊社の使えるクラウドバックアップは、業務委託は実施しておりませんが、社内規定により業務委託する際は守秘義務及び罰則規定について、委託契約書または秘密保持契約書にて明記することとなっております。
6					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。	弊社の使えるクラウドバックアップは、本リファレンスに定める運用管理規定を遵守し、「情報セキュリティ関連法」に従い定期的に関連法令等の遵守評価を実施しております。
7					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。	弊社の使えるクラウドバックアップは、情報処理の安全管理について、以下の経済産業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となっております。 ・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」 弊社の使えるクラウドバックアップは、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おります。 また、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
8						②	①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）	弊社の使えるクラウドバックアップは、本リファレンスを遵守状況としてホームページに掲載しており、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
9				(ウ)運用管理規程についての要求事項	1.基本方針と管理目的の表明	①	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。	弊社の個人情報保護指針はプライバシーポリシーに定め、ホームページ上に「プライバシーポリシー(https://www.tsukaeru.net/privacy)」を掲載して、個人情報の利用等について明示しております。 これらの条件を満たした運用管理規定や、必要な組織体制については文書化されており、ISO27001認証を継続して取得することで第三者の評価を得ております。
10						②	①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。	同上
11						③	①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。	弊社の使えるクラウドバックアップは、バックアップデータが医療情報であるかにかかわらず、データの中身について確認することはございません。 弊社にて生死を判別してデータを扱うことはできないため、死者に関する情報のデータであっても、通常の運用として扱っております。
12						④	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する。	弊社の情報セキュリティに関する基本方針は文書化し、ホームページ上に「情報セキュリティ基本方針(https://www.tsukaeru.net/security)」を掲載しております。 また、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っております。
13						⑤	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行う。	弊社では、最高技術責任者監督のもと、ISO事務局にて情報セキュリティポリシーの遵守を担保する組織体制を構築しており、 各部署と連携しながら、リスクアセスメント、セキュリティ教育、監査を実施する体制を文書化しております。
14						⑥	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き、医療機関等と合意する。	弊社では、本リファレンスを開示することで、医療機関等の担当者が弊社の情報セキュリティポリシーに合意できるかを判断できるようにしております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
15					2.サービス提供先の体制	①	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。	弊社の使えるクラウドバックアップは、24時間365日の監視体制となっており、障害発生時は迅速に対応しております。 また、お客様に提供しているサービスに影響のある障害発生時には、ホームページに状況を掲載するとともに、対象のお客様へメールでご連絡しております。 尚、お客様からの各種お問い合わせについてはサポート窓口（https://www.tsukaeru.net/support）にてお受けしております。
16						②	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスの体制に合意できるかを判断できるようにしております。
17					3.契 約 書・ 3.マニュアル等の文書の管理	①	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、これに基づき文書の管理を行う。	弊社の情報セキュリティに関する基本方針は文書化し、ホームページ上に「情報セキュリティ基本方針（https://www.tsukaeru.net/security）」を掲載しております。 また、ISO27001で策定したISMSマニュアルにて文書を管理しております。
18						②	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する。	同上
19						③	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の提供する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合意できるかを判断できるようにしております。
20						④	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き、医療機関等と合意する。	同上
21					4.リスクの発現の予防、発生時の対応の方法	①	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。	弊社の使えるクラウドバックアップは、サービスに係るリスク分析を「情報資産管理台帳」にてリスクアセスメントを実施し、必要な場合はリスク対応計画にて対応しております。 その運用品質についてはISO27001の外部認証を行い、定期的に第三者評価を受けることで担保されております。 また、様々なリスクの中でもお客様のご利用に影響がある故障・メンテナンス情報については速やかにホームページへの掲載やメール等で通知を行っております。 各種通知やサポートに関する詳細は以下を参照ください。 https://www.tsukaeru.net/support
22						②	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに係るリスク分析及び対応等について合意できるかを判断できるようにしております。
23					5.機器を用いる場合の機器等の管理	①	機器等の管理方法について、文書化を行う。	弊社の運用に必要な機器は管理台帳で用途や状況が管理されております。また社外に持ち出す情報機器については「持出持込記録」にて管理し、定期的に所在確認を実施しております。 その運用品質についてはISO認証により定期的に第三者評価を受けることで確保されております。
24						②	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。	同上
25						③	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の機器等の管理等に関する運用について合意できるかを判断できるようにしております。
26					6.個人情報の記録媒体の管理方法	①	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する。	弊社の記録媒体は「取外し可能記録媒体管理台帳」および「CD/DVD管理台帳」にて管理しております。 外部からの持込や社外への持出が必要な場合は申請を必要とし、「持出持込記録」にて管理しております。 シャトル便については「シャトル便管理台帳」に従い管理しております。
27						②	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の個人情報を記録した媒体の管理等に関する運用に合意できるかを判断できるようにしております。
28					7.患者等への説明と同意を得る方法	①	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、医療機関等で患者等への説明および合意を得るサービスに関しては提供していないため、対象外とさせていただいております。
29					8..監査	①	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、内容等について明文化を行う。	弊社の使えるクラウドバックアップは、運用等に関する文書化された規定及び体制の中で厳正に運用されております。 その適正性については定期的な内部監査、およびISOの外部監査によって第三者評価がなされております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
30						②	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は、これに対する監査又は代替する対応についての方針、内容を明確にする。	弊社の使えるクラウドバックアップは、自社でサービスを提供しておりますので、対象外とさせていただきます。
31						③	監査実施について記録し、当該記録の保存･管理方法を明確にする。	弊社では、内部監査実施について、「内部監査報告書」、外部監査については「審査結果報告書」の記録を保存しております。 また、監査で不適合となった項目については是正処置を実施して改善しております。 その運用品質についてはISO認証により定期的に第三者評価を受けることで確保されております。
32						④	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の実施する情報システム監査等について合意できるかを判断できるようにしております。
33						⑤	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の監査記録等の範囲･条件等について合意できるかを判断できるようにしております。
34					9.苦情・質問の受け付け窓口の設置	①	医療機関等の管理者からの問合せ窓口を設ける。また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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、医療機関等の管理者からのお問い合わせ窓口については、お電話、サポートメール、チャット、緊急連絡、FAQでお受けしております。 詳細は下記のお問い合わせ一覧をを参照ください。 https://www.tsukaeru.net/support また、本リファレンスを開示することで、医療機関等の担当者が弊社の受付時間等について合意できるかを判断できるようにしております。
35						②	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する。	弊社の使えるクラウドバックアップは、自社で提供しており、医療機関等からの問合せ窓口も自社で受け付けております。
36				(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	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る。	弊社の使えるクラウドバックアップは、特定の作業者のみのアクセスに限定し、2要素認証により不正アクセスを防止しております。 また、システムへのアクセス記録は保存されており、アカウントの追加･削除の管理および権限等の見直しを含めて定期的にレビューを実施しております。
37						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。	同上
38					2.委託契約に含めるべき事項	①	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。	弊社の使えるクラウドバックアップは、自社で運用管理しておりますので、委託は実施しておりません。
39			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	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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、従業員のみの入館で、セキュリティカード+暗証番号により施錠管理されております。 外来者は、従業員の立ち合いのもとで入館とし、機器への不正アクセスを防止しております。
40						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。	同上
41						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。	同上
42					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。	同上
43						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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、従業員のみの入館で、セキュリティカード+暗証番号により施錠管理されております。 また、入退管理システムおよび各出入口に設置された監視カメラにより入退者の特定が可能となっており、入退状況を定期的にレビューすることで、不正な入退を防止しております。
44						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。	同上
45						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。	同上
46						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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、個人所有物の持込が必要な際は申請を必要としており、「持出持込記録」にて管理しております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
47						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。	同上
48						⑦	①～⑥につき、運用管理規程等に規定する。	弊社の使えるクラウドバックアップは、運用管理規定等を本リファレンスにて規定しております。 また、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスの運用管理規定等に合意できるかを判断できるようにしております。
49					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。	弊社データセンターの災害対する状況は下記となっております。 ・地震：2008年建築基準により建築された施設であり、今までに地震による災害が発生したことのない安定した地盤に設置されております。 ・水害：市のハザードマップから外れた場所となり、今まで水害による被害が発生したことはございません。 ・落雷：避雷針を設置し、UPSから電源を供給することで落雷による影響はございません。 ・火災：コンピュータ機器類に影響のないアルゴン+窒素混合ガス消火設備を設置しており、火災発生時は煙検知システムにより自動検知して消火する仕様となっております。 ・停電：停電発生時は、UPS及び非常用発電装置により24h以上稼働できる燃料を常備しております。 ・結露：空調設備にも非常用発電装置から電力を供給できるため、停電時も通常の温度環境を維持することが可能となっております。
50						②	①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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、本リファレンスを開示することで、医療機関等の担当者が弊社の施設を設置する建築物に合意できるかを判断できるようにしております。
51					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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、不正な侵入を防ぐため、監視カメラをにより90日以上記録を保管としております。 また、不正な侵入を検知した場合に警備員が現場にかけつけるため、警備会社による自動侵入検知システムが設置されております。
52						②	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。	同上
53						③	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する。	同上
54				(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	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。	弊社の使えるクラウドバックアップは、データが医療情報であるかにかかわらず、バックアップデータの中身について閲覧することはございません。 医療機関等からの依頼により確認が必要な場合は、アクセス権限のないものが閲覧できない場所で作業をする手順としております。
55						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。	同上
56				(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事項	1.機器・媒体等の盗難・紛失防止	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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置して常時稼働しており、持出等による紛失はございません。 また、バックアップサーバーに保存されているデータは、個人情報が含まれるか否かにかかわらず、端末にデータを保存することは禁止しております。 尚、医療機関等から記録媒体を経由してバックアップデータを預かるシャトル便については、「シャトル便運用手順」に従って作業ログを管理し、「持出持込管理」にて定期的に所在確認を実施しております。
57						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。	同上
58						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。	同上
59			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	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）。	弊社の使えるクラウドバックアップは、運用管理関するアカウントは、作業者単位にすべてユニークなアカウントを利用しております。
60						②	利用者のなりすまし等を防止するための認証を行う。	弊社の使えるクラウドバックアップは、不正ログインによる利用者のなりすまし等を防止するため、2要素認証を採用しております。
61						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。	弊社の使えるクラウドバックアップは、運用管理における利用者は弊社で管理しており、医療機関等に提供しているサービスにおける利用者については、医療機関等の管理範囲となっております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
62						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の発行は必要最小限とし、定期的な棚卸しを行う。	弊社基盤の管理者、作業者については必要最低限のアカウント払い出しを行い、台帳管理を行って運用しております。各作業者等の異動や退職等にも迅速に対応するべく、定期的にレビューがなされており、その品質はISOにおいて定期的に第三者評価を受けております。
63					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。	弊社の使えるクラウドバックアップは、新規にアカウントを作成すると、最初のログイン時に初期パスワードを強制で変更を求めるようになっております。 また、弊社の従業員はパスワード管理システムを利用して各自ランダムなパスワード（英数字・大文字小文字・記号)を自動生成して設定しております。
64						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。	弊社の使えるクラウドバックアップは、パスワード入力を3回失敗すると再入力を一定時間受け付けない仕様となっております。
65						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。	弊社の使えるクラウドバックアップは、アカウントのパスワードについて2要素認証を採用しており、ログインのたびにパスワードとワンタイムパスワードを必要としております。 尚、患者等については、医療機関等の管理範囲となるため、対象外とさせていただいております。
66						④	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を確保する。	弊社の使えるクラウドバックアップは、2要素認証となっております。
67					3.パスワードの管理	①	利用者のパスワード情報は、ハッシュ値での保存を行う等、暗号化手法により、管理する。	弊社の使えるクラウドバックアップは、アカウントのパスワード情報は暗号化して管理されております。
68						②	サービスに供する製品等の導入に際しては、初期パスワードを変更するだけでなく、必要な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行う。	弊社の使えるクラウドバックアップは、従業員の人事異動等に合わせ権限やアカウントの棚卸を実施し、不要なアカウントを削除しております。
69						③	利用者がID、パスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。	弊社の使えるクラウドバックアップは、緊急障害発生時やパスワード失念などのインシデント等発生の際にも迅速かつ柔軟な対応ができるように、文書化された対応フローと体制の元で運用が行われております。医療機関等からの各種お問い合わせについてはサポート窓口においてお受けしております。 サポート窓口についての詳細は以下を参照ください。 https://www.tsukaeru.net/support
70						④	パスワード等の情報の漏洩が生じた場合又は不正な第三者からの攻撃により漏洩した場合には、直ちに当該IDを無効化し、あらかじ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する。	弊社の使えるクラウドバックアップは、弊社従業員のアカウントでパスワード等の情報漏洩が発生した場合、該当のアカウントを無効化した上で状況調査及び対策の実施となっております。 医療機関等のアカウントについては、医療機関等の管理範囲となるため、医療機関等で調査対応いただくこととなっております。 尚、医療機関等からの依頼により変更が必要な場合は、初期化できる仕組みとなっております。
71						⑤	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、当該パスワードを無効化し変更できるような対応を講じる。	同上
72						⑥	利用者が設定するパスワードについては、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行う。	弊社の使えるクラウドバックアップは、弊社従業員のアカウントについて、パスワード管理システムを利用して各自ランダムなパスワード（英数字・大文字小文字・記号)を自動生成して設定しております。 医療機関等のパスワードについては、医療機関等の管理範囲となるため対象外とさせていただいております。
73						⑦	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、安全性を確保するのに必要な範囲で、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行う。	同上
74						⑧	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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社のパスワードポリシーについて合意できるかを判断できるようにしております。
75					4.複数要素認証への対応	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。	弊社の使えるクラウドバックアップは、弊社従業員のアカウントについて2要素認証を必須としております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
76						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。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスの認証方式について合意できるかを判断できるようにしております。
77						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。	弊社の使えるクラウドバックアップは、利用者の認証において2要素認証を採用しております。
78						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。	弊社の使えるクラウドバックアップは、利用者の認証に際して物理的な媒体（ICカード等）の利用はないため、本項目については対象外となっております。
79						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。	同上
80						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。	同上
81						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。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスの一時的な利用者の認証方法について合意できるかを判断できるようにしております。
82				(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	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。	弊社の使えるクラウドバックアップは、データが医療情報であるかにかかわらず、バックアップデータの中身について閲覧することはございません。 弊社では、バックアップシステム全体のデータを医療情報として区分しアクセス制御して管理しております。
83						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。	同上
84						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。	弊社の使えるクラウドバックアップは、仮想化技術を用いたサービスを提供しておりませんので、本項目は対象外とさせていただいております。
85						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。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社の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合意できるかを判断できるようにしております。
86					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。	弊社の使えるクラウドバックアップは、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仕組みとなっております。
87						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。	弊社の使えるクラウドバックアップは、利用者の職種権限については、職位ならびに、管理者かどうか、という権限設定をするアクセス権限機能を提供しております。また、この設定については、利用者の管理画面から設定でき、医療機関は必要に応じて、医療機関内での運用に応じて設定をすることが可能となっております。システム利用者によるアクセス権限の定義については、本システムの操作マニュアルにて定義しており、本内容は利用者全てが確認可能となっております。なお、弊社では、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おります。
88						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。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社のアクセス管理について合意できるかを判断できるようにしております。 尚、医療機関等の内部のアクセス管理については、医療機関等の管理範囲となるため対象外とさせていただいております。
89					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。	弊社の使えるクラウドバックアップは、バックアップデータの中身について確認することはございません。 患者等の管理については医療機関等の管理範囲となるため、本項目は対象外とさせていただいております。
90				(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 1.PC 等の汎用入力端末により記録が作成される場合合	①	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	弊社の使えるクラウドバックアップは、バックアップサービスの提供となり、医療情報を含む文書等の作成については、医療機関等の管理範囲となるため対象外とさせていただいております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
91					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	①	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築に関する役割分担	同上
92					(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 PC 等の汎用入力端末により記録が作成される場合	①	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 ・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	同上
93					(c)更新履歴の保存に関する安全管理対策 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。	弊社の使えるクラウドバックアップはNotary機能でバックアップデータと原本を比較する仕組みがあります。
94					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。	弊社の使えるクラウドバックアップは、バックアップサービスの提供となり、医療情報を含む文書等の作成については、医療機関等の管理範囲となるため対象外とさせていただいております。
95					(d)代行入力の承認機能に関する安全管理対策	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。	同上
96						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。	同上
97						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)に関する機能を含める。	同上
98				(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	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。	弊社の使えるクラウドバックアップは、バックアップシステムへのアクセスについてアクセスを記録し、一定期間保持しております。 アクセス記録の項目については、アクセスしたID、時間、IP、ログイン方法、アクセス対象等 となっております。
99					アクセス記録の取得	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。	同上
100					アクセス記録の取得	③	ア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。	同上
101						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。	弊社の使えるクラウドバックアップは、医療機関等のバックアップデータを扱っており、中身のデータについては確認しておりません。 医療情報や診療録等の保存期間に関しては、医療機関等の管理範囲となるため対象外とさせていただいております。
102						⑤	④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。	同上
103					アクセス記録の取得	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。	弊社の使えるクラウドバックアップは、システム運用者のアクセス記録を保存しており、アカウントの追加･削除の管理および権限等の見直しを含めて定期的にレビューを実施しております。
104						⑦	⑥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。	弊社の使えるクラウドバックアップは、本リファレンスを開示することで、医療機関等の担当者が弊社のアクセス記録の管理について合意できるかを判断できるようにしております。
105					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て、アクセス制限を行い、不正なアクセスを防止する。	弊社の使えるクラウドバックアップは、アクセス記録の保存先について、特定の作業者のみアクセス可能となっております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
106						②	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。	弊社の使えるクラウドバックアップは、システムのアクセス記録の保存先について、容量監視を設定しており、容量不足が検知された場合は迅速に対応しております。
107						③	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。	弊社の使えるクラウドバックアップは、システムのアクセス記録を暗号化により改竄防止しており、ログローテーションにより管理しております。
108					3.時刻の設定	①	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行う。	弊社の使えるクラウドバックアップは、システムのアクセス記録の保存先にNTPを設定しており、常に同期されております。
109				(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	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。	弊社は、ISO27001の適用宣言書にてクリアデスク･クリアスクリーン方針の規定を定めており、定期的にチェックを実施しております。 尚、弊社の使えるクラウドバックアップは、バックアップデータの中身が医療情報であるか否かにかかわらず、バックアップデータの中身について閲覧することはございません。
110						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。	弊社の使えるクラウドバックアップは、自社データセンターに機器を設置しており、監視カメラにより監視されております。 バックアップシステムにアクセスする端末は監査サーバーを経由することで操作ログを記録しており、2要素認証により端末からの不正なアクセスを防止しております。
111						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。	弊社の使えるクラウドバックアップでは、医療機関等に設置されている医療情報については、医療機関等の管理範囲となるため対象外とさせていただいております。
112						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。	同上
113						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。	同上
114				(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	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。	弊社の使えるクラウドバックアップは、システム構築に際して使用する端末について、社内規定ウイルススキャンソフトのインストールを必須としております。 また、社内端末のウイルススキャンソフトを集中管理することで、定義ファイルやセキュリティパッチの適用状況を管理し、常に最新の状態に更新することで、構築したシステムへのウイルスやマルウェア等の混入対策としております。
115						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。	同上
116						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。	同上
117						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。	弊社の使えるクラウドバックアップは、弊社の運用端末がウイルス等による攻撃を受けた場合、端末の利用者はISO2701で規定されたルールに沿ってエスカレーションし、サービス提供に影響がある場合、速やかに医療機関等へ連絡し必要な対応等を実施することとなっております。 また、医療機関等の端末がウイルス等による攻撃を受けた場合については、医療機関等の管理範囲となるため対象外とさせていただいております。
118						⑤	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、確認する。	弊社は、脆弱性に関する情報について、独立行政法人情報処理推進機構（IPA）を定期的に確認しております。 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おります。
119					2.外部からの攻撃等への対策	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。	弊社の使えるクラウドバックアップは、外部のネットワークからのアクセスにおいてゲートウェイサーバーを経由する仕組みとなっております。 ゲートウェイサーバーにより接続先を限定し、弊社の運用ルールに沿ってアクセス制御を行っております。
120						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。	弊社の使えるクラウドバックアップは、医療機関等からのアクセスについて、Firewallで必要なポートのみ通しており、監視システムで異常なトラフィックを検知した場合、攻撃・不正アクセス等がないかについて調査対応しております。
121						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。	同上
122						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にて、同様の制御を行う。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
123				(キ)応答時間に関する要求事項		①	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。	弊社の使えるクラウドバックアップは、バックアップ時間について、医療機関等の回線や機器のスペック、データの更新頻度等に依存するため、環境により所要時間が異なっております。 バックアップ時間について、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
124				(ク)医療情報等の保存に対する要求事項	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。	弊社の使えるクラウドバックアップは、各医療機関等からコントロールパネルにアクセスすることで、利用可能な残容量について確認頂けるシステムとなっております。
125						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。	弊社の使えるクラウドバックアップは、バックアップデータの保存可能な容量、その他オプションについて弊社ホームページに記載しており、 医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
126						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。	弊社の使えるクラウドバックアップは、医療機関等の担当者がコントロールパネルにアクセスすることで、保存場所、保存期間、保存容量について調整が可能となっております。 バックアップのポリシーに関する運用管理規定等については、医療機関等の管理範囲となるため対象外とさせていただいております。
127						④	③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。	弊社の使えるクラウドバックアップは、自社データセンターに設置してある機器にてサービスを提供しておりますので、本項目は対象外とさせていただいております。
128						⑤	③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。	弊社の使えるクラウドバックアップは、医療機関等の担当者がコントロールパネルにアクセスすることで、医療機関等にてデータを管理可能となっておりますので、バックアップの運用管理および教育については、医療機関等の管理範囲となるため対象外とさせていただいております。
129						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。	同上
130					2.バックアップルール	①	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。	弊社の使えるクラウドバックアップは、医療機関等の担当者がコントロールパネルにアクセスすることで、医療機関等でバックアップの運用管理が可能となっております。 バックアップの取得対象、取得頻度などについては、医療機関等の管理範囲となるため対象外とさせていただいております。
131						②	①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。	同上
132						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。	同上
133						④	③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。	同上
134						⑤	①～④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。	同上
135						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。	同上
136					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。	医療機関等に設置されている情報システム、ネットワーク等については、医療機関等の管理範囲となるため対象外とさせていただいております。 弊社の使えるクラウドバックアップは、バックアップシステムに用いる機器を冗長化して構築しております。
137						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。	同上
138						③	①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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、バックアップシステムに障害等が生じた場合、弊社の運用手順に従い対応を実施しております。 また、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。 尚、医療機関等に設置された機器の障害対応については、医療機関等の管理範囲となるため対象外とさせていただいております。
139						④	障害時等でも診療等が継続できるよう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き、医療機関等と合意する。	弊社の使えるクラウドバックアップは、障害時等でもサービスが提供できるよう冗長化されております。 尚、医療機関等に設置された機器の障害等については、医療機関等の管理範囲となるため対象外とさせていただいております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
140					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。	弊社の使えるクラウドバックアップは、バックアップデータが暗号化された状態で保存されており、データの中身の状態については医療機関等の管理範囲となるため、対象外とさせていただいております。 バックアップから特定のデータを復旧する場合も、医療機関等の担当者がコントロールパネルにアクセスすることで対応が可能となっておりますので、医療機関等の管理範囲となるため対象外とさせていただいております。
141						②	①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。	同上
142						③	②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き、医療機関等と合意する。	同上
143					5.保存データの見読性確保	①	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する。	弊社の使えるクラウドバックアップは、バックアップデータが暗号化された状態で保存されており、データの中身の状態については医療機関等の管理範囲となるため、対象外とさせていただいております。 バックアップから特定のデータを復旧する場合も、医療機関等の担当者がコントロールパネルにアクセスすることで対応が可能となっておりますので、医療機関等の管理範囲となるため対象外とさせていただいております。
144						②	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、見読性確保のための対応を行う。	同上
145				(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	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。	弊社の使えるクラウドバックアップはサービス提供に必要な各種設定基準を文書化し運用しております。医療機関等に設置されている情報システムの構成等については、医療機関等の管理範囲となるため対象外とさせていただいております。
146						②	情報システムのネットワーク構成図を作成する。	同上
147						③	①、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。	同上
148						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。	弊社の使えるクラウドバックアップは、バックアップサービスに用いる機器の構成および更新について管理しております。 尚、医療機関等に設置されている情報システムの構成や更新仕様等については医療機関等の管理範囲となるため対象外とさせていただいております。
149						⑤	①～④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。	弊社の使えるクラウドバックアップは、システム構成について、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。 弊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おります。
150					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。	弊社の使えるクラウドバックアップは、サービスの品質を維持･管理し、故障発生時には早期に復旧させ、お客様への影響を最小限にするよう定めております。 又、基盤環境を管理･提供する担当者へは教育計画プログラムを実施し品質強化を図っております。
151						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。	同上
152						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。	サービス委託先がないので対象外とさせていただいております。
153						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める。	弊社のサービスの品質を維持･管理するために運用管理手順はISO事務局により定期的に内部監査する手順が規定され実施しております。 また、保守作業が実施される場合はメンテナンス日時を事前にアナウンスし、停止時間を最小限にとどめて保守作業を実施しております。
154				(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	①	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。	医療機関等にによるアクセス方式については、医療機関等の管理範囲となるため対象外とさせていただいております。 また、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
155					2.IoT 機器を利用したサービス提供時	①	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、サービス仕様適合開示書に基づき、医療機関等と合意する。	同上
156						②	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する。	同上
157						③	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。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
158			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	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。	弊社の就業規則にて守秘義務に関する規定を定めております。また従業員は入社時に「入社時誓約書」「秘密保持および個人情報に関する誓約書」にサインして同意しております。 また、定期的にセキュリティ教育を実施することで従業員のセキュリティ意識の向上を図っております。
159					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。	同上
160						②	この教育・訓練は就業開始時及び就業後定期的に行う。	同上
161					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。	弊社の就業規則にて守秘義務に関する規定を定めております。また従業員の退職時は「退職時誓約書」ににサインして、退職後も守秘義務に同意しております。 また、定期的にセキュリティ教育を実施することで従業員の退職後のセキュリティ意識の向上を図っております。 退職時には、「資産貸出返却リスト」にて個人情報にアクセスできるアカウントの返却、削除を実施しております。
162						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。	同上
163						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。	同上
164					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。	守秘義務違反者への罰則については、「就業規則」および「秘密保持及び個人情報に関する誓約書」に規定されております。
165					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・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き、医療機関等と合意する。	弊社の教育訓練の実施状況や守秘義務等への対応状況等について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
166				(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	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。	サービス委託先がないので対象外とさせていただいております。
167						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。	同上
168						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。	同上
169						④	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する。	同上
170						⑤	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する。	同上
171			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	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。	弊社の使えるクラウドバックアップ機器等の情報記録媒体の破棄については、「情報記録媒体の処分手順」に従って処理しております。
172						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。	情報記録媒体の破棄については、「廃棄リスト」にて管理しており、医療機関等の求めに応じて情報を報告させていただきます。
173						③	①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。	弊社の情報記録媒体の廃棄手順等について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
174					2.情報破棄手順の文書化	①	①運用管理規定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）。	弊社の使えるクラウドバックアップ機器等の情報記録媒体の破棄については、「情報記録媒体の処分手順」に従って処理しております。
175						②	② 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き、医療機関等と合意する。	弊社の情報記録媒体の廃棄手順等について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
176			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	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。	弊社基盤の管理者、作業者については必要最低限のアカウント払い出しを行い、台帳管理を行って運用しております。各作業者等の異動や退職等にも迅速に対応するべく、定期的にレビューがなされており、その品質はISOにおいて定期的に第三者評価を受けております。
177						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。	弊社運用環境に対するアクセスに関しては文書化された運用定義書によってログ取得を義務付けており、アカウントを払い出された職員のみがアクセスできる運用を行っております。ログイン等のログ情報は全て管理され保存されております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
178					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しないよう厳重に管理する。	弊社基盤の管理者、作業者については必要最低限のアカウント払い出しを行い、台帳管理を行って運用しております。各作業者等の異動や退職等にも迅速に対応するべく、定期的にレビューがなされており、その品質はISOにおいて定期的に第三者評価を受けております。
179				(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	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。	弊社メンテナンス業務におけるサービス機器へのアクセスはリモートアクセスを原則としており、バックアップシステムにアクセスする端末は監査サーバーを経由することで操作ログを記録しております。 また、すべての作業実施内容は文書化されたワークフローにおいて定義されており不審な操作の定期的なレビューが行われております。
180						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。	同上
181						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。	弊社のメンテナンス実施に関する安全管理対策について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
182					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。	弊社のメンテナンス業務においては、すべての操作ログを記録しており不審な操作の定期的なレビューが行われております。
183						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。	同上
184					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。	弊社のメンテナンス実施に関する安全管理対策について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
185					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。	弊社バックアップサーバについては、脆弱性やバグが生じた際に、あらかじめ指定されたいるメンテナン方法でメンテナンスを実施しております。その際、メンテナンスの内容によっては、通信断が生じることもありますがお客様には事前通知いたします。 お客様のサービスご利用にあたってのシステム運用状況、工事・メンテナンス情報については最新版をWebサイトにおいて常時公開しております。その他のお問い合わせについてはサポート窓口にてお受けしております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
186						②	①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合を想定して原状回復に必要な時間の予測を含める。	同上
187						③	保守業務の実施にあたっては、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。	同上
188						④	③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き、医療機関等と合意する。なお、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き、医療機関等と合意する。	同上
189						⑤	④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き、医療機関等と合意する。	同上
190						⑥	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き、医療機関等と合意する。	同上
191				(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	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。	弊社メンテナンスに用いるデータでは、受託医療機関のデータの利用は禁止されており、弊社で作成したテストデータをもとに実施しております。
192						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。	同上
193						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。	同上
194					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。	弊社データセンターではデータが入った記憶媒体のサーバ室外への持出は禁止されております。記憶媒体をサーバ室から持ち出す場合には記憶媒体の物理破壊を行う為、利用者の情報がサーバ室外へ持ち出されることはございません。
195						②	①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。	同上
196				(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	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。	弊社の使えるクラウドバックアップは、バックアップサービスの提供となり、医療情報を含む文書等の作成については、医療機関等の管理範囲となるため対象外とさせていただいております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
197						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。	同上
198					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。	弊社の使えるクラウドバックアップサービスに関するマスターデータの変更がある場合 は、事前に変更内容をテスト環境で検証した上で実施しております。医療情報に係るマスターテーブルの変更ついては、医療機関等の管理範囲となるため対象外とさせていただいております。
199						②	①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。	同上
200					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。	弊社の使えるクラウドバックアップサービスに関するデータ形式や転送プロトコルの変更がある場合 は、事前に変更内容をテスト環境で検証した上で実施しております。なお、利用する医療機関はそのことを意識することなくご利用いただけます。
201						②	①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。	弊社の使えるクラウドバックアップサービスの変更において利用する医療機関に影響を及ぼす場合は、双方で仕様を十分すり合わせた上で実施させていただきます。提供しているサービスが終了する場合は、医療機関に弊社サービスの機能停止、データ削除等の作業を実施いただきます。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
202						③	②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。	同上
203						④	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。	同上
204					4.サービスに供する機器の劣化対策	①	サービスに供する情報システムに関する機器については、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。	弊社の機器においては定期的に買い替えを行うとともに、セキュリティや脆弱性の見直しがされており、更新の際には、サービス品質へ影響が発生しないように検証を行った上で導入を行っております。 又、ISO27001等、ITシステム運用に必要な認証を取得し、定期的に外部を受けることでその品質を確保しております。
205						②	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は、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。	弊社の使えるクラウドバックアップサービスの変更において利用する医療機関に影響を及ぼす場合は、双方で仕様を十分すり合わせた上で実施させていただきます。提供しているサービスが終了する場合は、医療機関に弊社サービスの機能停止等の作業を実施いただきます。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
206						③	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には、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。	同上
207						④	③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き、医療機関等と合意する。	同上
208					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	①	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は、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を行う。	弊社の使えるクラウドバックアップサービスの変更において利用する医療機関に影響を及ぼす場合は、双方で仕様を十分すり合わせた上で、互換性確保または標準仕様の変化への対応を図っております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
209						②	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には、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するための対応策を検討し、対策を講じ る。なお、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）等が生じる場合には、「4. サービスに供する機器の劣化対策」②～④に示す対応策を講じる。	他社のクラウドサービス利用がないので対象外とさせていただいております。
210						③	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、又は利用する他の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には、①、②を考慮して行う。	弊社の使えるクラウドバックアップサービスの変更において利用する医療機関に影響を及ぼす場合は、双方で仕様を十分すり合わせた上で、互換性確保または標準仕様の変化への対応を図っております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
211				(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	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。	弊社の保守業務においてはその作業は品質を確保すべく文書化されており、担当者等に依存しないように運用管理されております。その適正性については定期的な内部監査、およびISOの外部監査によって第三者評価がなされております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
212					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。	再委託先がないので対象外とさせていただいております。
213						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。	同上
214			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	①	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。	弊社の情報処理装置を持ち出す場合は、運用管理規程のISO申請書により申請し、持出持込管理の台帳で管理しております。 持出機器は紛失が発生しないよう定期的にチェックしております。
215						②	①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む。	弊社のバックアップサービスにおいて、ネットワークを通じたバックアップデータの外部への送信等はございません。
216						③	①で定める内容について、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。	弊社の情報記録媒体の持出し等について、本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
217					2.サービスに供する記録媒体・記録機器に関する対応	①	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む。） ・サービスに関する情報を持ち出した場合で、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、暗号化、ファイアウォール導入等））	弊社の情報処理装置を持ち出す場合は、運用管理規程のISO申請書により申請し、持出持込管理の台帳で管理し機器の紛失が発生しないよう定期的にチェックしております。 持出機器について紛失等の問題が発生した場合は、速やかに上長またはCTOへ連絡し指示を仰ぐとともに、「トラブル対応報告書」にて状況を記録し再発防止策を実施します。 保守運用業務におけるサービス機器へのアクセスはリモートアクセスを原則としており、予め定義された居室、端末およびネットワークを介して接続され、持ち出しによる情報漏洩等のリスク対策を実施しております。
218					3.従業員等及び委託先に対する対応	①	「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。	弊社の従業員は入社時にセキュリティ教育を実施し、情報記録媒体の持出しについても教育しております。 また、定期的に情報セキュリティ教育を実施することで従業員のセキュリティ意識の向上を図っております
219						②	上記の運用管理規程については、再委託先に対しても遵守等を求める。	再委託先がないので対象外とさせていただいております。
220					4.医療機関等との合意	①	「2.サービスに供する記録媒体・記録機器に関する対応」、「3.従業員等及び委託先に対する対応」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き、医療機関等と合意する。	弊社の情報記録媒体の取り扱いや従業員及び委託先に対する対応について、本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
221				(イ)機器・媒体の台帳管理		①	サービスに関する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。	弊社の使えるクラウドバックアップサービスに関する機器は「情報端末管理台帳」「取り外し可能記録媒体管理台帳」「持出持込記録台帳」で管理しております。 定期的に紛失が発生しないよう定期的にチェックしております。 その運用品質についてはISO認証により定期的に第三者評価を受けることで確保されております。
222				(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	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。	弊社の使えるクラウドバックアップサービスで利用頂く機器は24H常時稼働な為、起動パスワードの設定はしておりません。 なお、弊社の作業端末については2要素認証を採用しております。 医療機関の初回Backupデータを想定した「使えるシャトル便」として媒体を物理的に配送するサービスがありますが、データは暗号化されて格納しております。
223						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。	同上
224						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。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
225					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。	弊社の作業端末については2要素認証でアクセスする仕組みとなっております。 また、使えるクラウドバックアップサービスで利用頂く「使えるシャトル便」はバックアップデータを保存する際に自動的に暗号化する仕組みとなっております。 また、シャトル便の詳細な運用手順は「シャトル便運用手順」に記載しております。
226					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。	弊社の作業端末については、決められたアプリケーション以外インストールしないないように定期的にチェックしております。 また、「使えるシャトル便」においても必要最低限のアプリケーションがインストールされいるか持出・持込時にチェックしております。
227						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。	同上
228					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。	弊社の従業員が利用する情報機器については、原則として個人所有物の持込を禁止しております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
229						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。	同上
230					5.公衆無線LAN の利用禁止	①	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には、公衆無線LANへの接続は行わない。	弊社ではバックアップサービスの運用に使用する端末から公衆無線LANを利用してアクセスすることはありません。 社外で作業端末を利用する場合VPNで暗号化されたネットワークを使用してアクセスしております。
231			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	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。	弊社は障害発生時の責任分解として、サービスレベル合意書(SLA)にてサービス対象範囲および稼働保証を明示しております。なお、サービスレベル合意書（SLA）の適用は利用規約で明示されております。
232					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。	弊社の使えるクラウドバックアップサービスでは、医療情報は医療機関等に保存頂く事は推奨しておらず、クラウド基盤上に保管することを推奨しております。また、クラウド基盤は冗長化されデータ自体は3台の機器に保存する仕組みとなっております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
233					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。	同上
234					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。	同上
235					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づき、医療機関等と合意する。	同上
236				(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	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。	弊社の使えるクラウドバックアップサービスでは、災害時には保管場所を国内の別施設に変更して頂く事で再度利用できるようにしております。 弊社ではISO 27001 に準拠して事業継続管理規程を設けており、非常時における規程も含まれております。規程には「非常時におけるエスカレーション」、「関連部門への周知と指示」、「特別体制の整備」、「公的機関との連携」、「対象者への通知」が規定されております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
237						②	①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。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
238						③	①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。	同上
239					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。	弊社サービスではシステム障害等の非常時に用いる利用者アカウントは存在しません。また、全ての操作を行うことが可能な特権 ID は原則利用禁止としており、パスワードも当社の限られた管理者のみが把握している状況です。緊急時において特権 ID を利用する必要が生じた場合は、必要分のみ申請フロー発行され、作業終了後に、作業内容を検証し、本来行うべきでない作業を行っていないかを点検しております。作業終了後には、管理者がパスワードを適時に変更することで、不適切な特権 ID の利用が発生しないようにしております。
240						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。	同上
241						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。	同上
242						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。	同上
243					3.サイバー攻撃等への対応	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。	弊社運用環境に対するアクセスに関しては文書化された運用定義書によってログ取得を義務付けており、不審なアクセス等について定期的なレビューが行われております。また、万が一のインシデント等発生時の対応プロセス、体制、手順を定めており、迅速かつ適切な対応を徹底しております。
244						②	①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。	弊社は緊急時やインシデント等発生の際にも迅速かつ柔軟な対応ができるように、文書化された対応フローと体制の元で運用が行われております。お客様からの各種お問い合わせについてはサポート窓口においてお受けしております。 サポート窓口についての詳細は以下を参照ください。 https://www.tsukaeru.net/support なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
245						③	①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。	同上
246						④	③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。	弊社基盤は国内に設置されており、全て日本国内に保管されております。
247					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･検証方法の規定等）を講じる。	システム障害またはサイバー攻撃時に、何かしらの理由で医療機関等から受託する医療情報に欠損や不整合等が発生した場合は、該当する医療機関に対して、直前のバックアップデータに基づく復旧サービスを提供することとしております。本件に関する当社の責任範囲については、当社サービスの利用規約に記載しております。
248			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	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。	弊社のバックアップサービスの運用のために使用する機器はVPN接続経由でのアクセスとなっており暗号化された通信経路のため情報の盗聴、改竄から保護されております。 また、医療機関等が弊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おります。
249						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。	弊社サービスは、TLS1.2証明書を相互（お客様、弊社）で実施することで、アクセス先のなりすまし等の対策を講じていおります。
250						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。	弊社のバックアップサービスの運用のために使用する機器はVPN接続経由でのアクセスとなっております。 経路の安全性についてのネットワークへの対応等及びその条件等は、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
251						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。	弊社のバックアップサービスのネットワーク経路における役割の範囲については、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
252						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。	医療機関等の施設からインターネットへの経路は、弊社責任範囲外とさせて頂いておりますが、必要であればVPN接続を利用いたサービスの提供も可能となります。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
253					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。	お客様環境から弊社へ接続するネットワークはお客様にて管理・運用いただく必要があります。また、弊社ではアクセス制御機能としてアカウントの準備、認証、アクセス権の承認、アクセス権の削除をお客様にて実施していただく事が可能となっております。 医療機関等が弊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おります。
254						②	①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行う。	同上
255						③	①について、事業者が保守業務を再委託している場合には、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。	再委託先がないので対象外とさせていただいております。
256						④	厚生労働省ガイドライン第5版6.11 C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き、医療機関等と合意する。	弊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、対象外とさせていただいております。 なお、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
257					3.ネットワーク経路対応に用いる機器	①	ルータ等のネットワーク機器は、ISO15408で規定され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する。	弊社のバックアップシステムに使用しているNetwork機器は、ISO15408で規定されているセキュリティーターゲットに適合しております。 また、機器をリプレースする際も適合していることを条件に選定しております。
258						②	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き、医療機関等と合意する。	医療機関等の施設内のルータについては、医療機関等の主管範囲とさせて頂いているため、対象外とさせていただいております。。 医療機関等の施設内については医療機関等の管理範囲となることを、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
259					4.暗号化対策	①	送信元と相手先の当事者間で情報そのものに対する暗号化等のセキュリティ対策を実施する。	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おります。また、バックアップデータ自体も暗号化しております。
260						②	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。	同上
261						③	②のほか、メールの暗号化（S/MIME等）やファイルの暗号化への対応を医療機関等が求める場合には、その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き、医療機関等と合意する。	弊社が医療機関等に提供しているサービスはバックアップサービスとなります。 バックアップサービスにおいて、バックアップデータ自体が暗号化されている点について、本リファレンスを開示することで医療機関等の担当者が弊社の提供するサービスに合意できるかを判断できるようにしております。
262					5.通信経路の暗号化対策	①	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は、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の高い「高セキュリティ型」に準じた適切な設定を行う。	弊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おります。
263						②	SSL-VPNは、原則として使用しない。	弊社サービスでは、原則としてSSL-VPNは使用していません。
264						③	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、適切な対策を実施する。	弊社のバックアップシステムに接続する作業端末は、集中管理されたウイルススキャンソフトを必須としており、作業端末への不正なアクセスによる回り込みの対策としております。
265						④	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提供を行う。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き、医療機関等と合意する。	医療機関等には弊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、セッション間の回り込みに対する対策としています。なお、本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
266					6.回線の品質等	①	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き、医療機関等と合意する。	弊社の回線は、2系統の別プロバイダを利用することにより冗長化されております。 弊社サービスの回線品質については、本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
267					7.医療機関等の外部からのサービス利用	①	医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担等につき、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。	医療機関内の環境に関するため、対象外とさせていただきます。なお、医療機関等の端末利用上の制限は特に設けておりません。 なお、本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
268				(イ)保守における通信上の安全管理対策		①	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。	弊社保守運用業務における安全管理措置としてリモートメンテナンスはアクセス経路、アクセス方法、プロトコルアクセスは予め定義しております。また、情報にアクセスする権限を持つ作業者を最低限に抑えるようアクセス権を統制しております。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
269				(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	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。	お客様環境から弊社へ接続するネットワークはお客様にて管理・運用いただく必要があります。 なお、保管データは、お客様が所有・管理されるものであり、弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることはありません。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
270						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。	同上
271						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。	お客様環境に関するため、対象外とさせていただきます。
272					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。	弊社サービスは、直接的に医療機関等の患者へのデータアクセスは一切許可していないため、本事項は対象外とさせていただきます。
273						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。	同上
274						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、医療機関等と合意する。	同上
275			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		①	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に、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。	弊社サービスは、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。 法令で署名又は記名・押印が義務付けられた文書等 は、お客様が所有・管理されるものであり、弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることはありません。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
276						②	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には、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き、医療機関等と合意する。なお、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き、医療機関等と合意する。	同上
277						③	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には、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き、医療機関等と合意する。	同上
278				(イ)タイムスタンプの付与		①	電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、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き、医療機関等と合意する。	弊社サービスは、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。法令で署名又は記名・押印が義務付けられた文書等 は、お客様が所有・管理されるものであり、弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることはありません。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
279						②	タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの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き、医療機関等と合意する。	同上
280						③	タイムスタンプを付与した情報を取り扱う場合に、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き、医療機関等と合意する。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
281				(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		①	タイムスタンプを付与した情報を取り扱う場合に、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き、医療機関等と合意する。	同上
282		3．3 外部保存に関する要求事項	3.3.3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	(2)クラウドサービス事業者への要求事項	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	①	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。	弊社のバックアップサービスの運用のために使用する機器はVPN接続経由でのアクセスとなっており暗号化された通信経路のため情報の盗聴、改竄から保護されております。 また、医療機関等が弊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おります。
283						②	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。	同上
284						③	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。	弊社保守運用業務におけるサービス機器へのアクセスはリモートアクセスを原則としており、またすべての作業実施内容は文書化されたワークフローにおいて定義され、事前にレビューされます。また、実際の作業実施に関わるログについては取得管理し、異常検知時はアラート通知がなされることになっております。
285			3.3.4見読性の確保に関する要求事項	(2)クラウドサービス事業者への要求事項	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	①	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。	弊社のバックアップサービスでは保管データはお客様が所有・管理されるものであり、弊社では、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることはありません。
286						②	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。	同上
287						③	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。	同上
288						④	システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（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すること。	お客様環境に関しては,お客様ご自身で管理頂くため、、対象外とさせていただきます。 弊社基盤のシステム及び物理機器は故障に備えて冗長構成として設計・運用されております。
289						⑤	緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。	弊社のバックアップサービスでは保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり対象外とさせていただきます。 弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることは致しません。
290						⑥	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受託する機関の障害等に対応できるような措置を行っておくこと。	同上
291			3.3.5保存性の確保に関する要求事項	(2)クラウドサービス事業者への要求事項	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	①	保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、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しなくてはならない。	弊社サービスの変更を行う場合がありますが、以前のデータ形式を維持いたします。この場合のお客様に対する通知ポリシー等はサービス利用規約に則って運用されます。
292						②	ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。	弊社では、開発・運用端末は定期的な買い替えを行うとともに、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おります。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行った上で導入を行っております。これらの取り組みを通して、弊社サービス環境上、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おります。
293						③	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こと。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
294			3.3.6真正性の確保に関する要求事項	(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		①	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	弊社はそのサービス品質を確保すべく、厳しい社内ルールを策定し、運用を行っております。お客様の個人情報を適切に管理するためにプライバシーポリシーを策定しております。その他情報セキュリティに関する部分ではISO27001の認証を継続して取得、第三者による監査を受けることでその実効性を確保しております。 弊社の財務の信頼性については、財務諸表等は公開していませんが信用調査機関には登録されております。 プライバシーポリシー、および各種取得認証情報については以下を参照ください。 https://www.tsukaeru.net/privacy
295				(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	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。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることは致しません。
296						②	①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。	同上
297						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。	同上
298						④	①～③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②、③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。	同上
299					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。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社は、保管データの内容を把握することはできず、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることは致しません。
300						②	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。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社は、保管データの内容を把握することはできず（データは暗号化されて保管）、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることは致しません。
301				(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	①	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。	弊社では、受託した医療情報の解析・分析サービス、及び第三者提供サービスを提供していないため、本事項は対象外とさせていただきます。
302						②	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。	同上
303					2..受託情報の解析等の第三者提供制限	①	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。	弊社では、受託した医療情報の解析・分析サービス、及び第三者提供サービスを提供していないため、本事項は対象外とさせていただきます。
304						②	①の内容を、サービス提供に係る契約に含める。	同上
305						③	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）を行う場合には、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。	同上
306						④	③により、第三者提供（閲覧）を行う場合には、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･削除できる対応を行う。	同上
307						⑤	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には、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）の報告を行う。	同上
308						⑥	①～⑤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き、医療機関等と合意する。	同上

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
309			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		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。	弊社の個人情報保護指針はプライバシーポリシーに定め、ホームページ上に「プライバシーポリシー(https://www.tsukaeru.net/privacy)」を掲載して、個人情報の利用等について明示しております。 これらの条件を満たした運用管理規定や、必要な組織体制については文書化されており、ISO27001認証を継続して取得することで第三者の評価を得ております。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
310				(イ)外部保存実施に関する患者への説明		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。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社は、保管データの内容を把握することはできず（データは暗号化されて保管）、お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることは致しません。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
311		3．4 クラウドサービスの利用終了に関する要求事項	3.4.1クラウドサービスの利用終了における対応		クラウドサービス事業者への要求事項	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。	弊社基盤設備については、脆弱性やバグが生じた際に、あらかじめ指定されたいるメンテナン方法でメンテナンスを実施しております。その際、メンテナンスの内容によっては、通信断が生じることもありますがお客様には事前通知いたします。 サービスの一部機能の提供を廃止するときで、あらかじめ契約者に対してその廃止する機能の代替となる手段又は同等の機能を提示できない場合、3ヶ月前の予告期間をもって変更のサービス内容を通知いたします。'お客様のサービスご利用にあたってのシステム運用状況、工事・メンテナンス情報についてはWebサイトにおいて常時公開しております。その他のお問い合わせについてはサポート窓口にてお受けしております。 https://www.tsukaeru.net/support
312						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。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社では契約終了後、一定期間後に弊社データセンターで削除処理される仕様となります。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
313						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。	同上
314						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。	弊社サービスの一部機能の提供を廃止するときで、あらかじめ契約者に対してその廃止する機能の代替となる手段又は同等の機能を提示できない場合、3ヶ月前の予告期間をもって変更のサービス内容を通知いたします。 本リファレンスを開示することで医療機関が合意できるか判断できるようにしております。
315						⑤	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、②、③に示す対応策を講じる。	保管データ（お客様がクラウドサーバ上にアップロード・保管されるデータをいおります）をアップロード・保管するリージョン/サイクルは自由に選択できます。保管データについてはお客様が所有・管理されるものであり本項目は対象外とさせていただきます。 弊社では契約終了後、一定期間後に弊社データセンターで削除処理される仕様となります。
316						⑥	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は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。	医療機関等からバックアップデータの削除依頼があった場合は、削除を行った記録を提出いたします。
317						⑦	⑥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、記録を保持し続ける場合には、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き、医療機関等と合意する。	弊社では契約の解除等があったときは、契約者データを削除すると明示されおり、弊社のサービス解約時後に記録を保持し続けることがないため対象外とさせていただきます。

Seq.	「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）」で必要とされる実施事項							
	省	節	段	項	小項目	番号	要求事項	対応状況
318						⑧	①～⑦についての手順等を、運用管理規程等に含める。	弊社の使えるクラウドバックアップサービスの利用終了における対応方針については、運用管理規定等を本リファレンスにて規定しております。 また、本リファレンスを開示することで、医療機関等の担当者が弊社の提供するサービスの運用管理規定等に合意できるかを判断できるようにしております。
319		3．5 オンライン診療システム提供事業者における安全管理対策	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		医療機関に対するオンライン診療におけるセキュリティ情報の要求事項を踏まえ、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の要求事項を以下に示す。			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(データ本体のバックアップサービス)ため、本項目は対象外とさせていただきます。
320		3．6 PHR サービス事業者における安全管理対策			医療機関等が管理する医療情報を取り扱うクラウドサービス事業者に対する要求事項のうち、読み替えて PHR サービス事業者に適用する要求事項を下記に示す。			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(データ本体のバックアップサービス)ため、本項目は対象外とさせていただきます。