病院経営プラットフォーム「ここりんく」
サービス仕様適合開示書

株式会社プレアデスセブン

（2023年2月　初版）

目次

1. 医療機関等が医療情報安全管理ガイドラインに基づき、外部保存を受託する事業者の 選定にあたり最低限確認する必要がある内容

（1） 医療情報等の安全管理に係る基本方針・取扱規定等の整備状況

■個人情報のお取り扱いについて：https://www.pleiades7.co.jp/privacypolicy/

（2） 医療情報等の安全管理に係る実施体制の整備状況

■管理責任者 ： 代表取締役

■システム管理者 ： 開発部マネージャ

■運用管理責任者 ： 開発部マネージャ

■個人情報保護責任者 ： 開発部マネージャ

（3） 実績等に基づく個人データ安全管理に関する信用度

これまでに、個人情報の流出事故はありません。

また、受託情報の目的外利用、不当利用等も行っておりません。

（4） 財務諸表等に基づく経営の健全性

■当社の電子公告・決算公告

出資受入について：https://www.pleiades7.co.jp/news/2009/

2. 医療機関等との共通理解を形成するために情報提供すべき内容

（１）医療機関等の運用管理規程に定める必要がある事項

次の事項に関しては、本サービスを利用する医療機関様にて、管理規程を定めてください。

□ 本サービスを利用する場所に関する事項（作業場所の特定、作業場所のアクセス制限など）

□ 本サービスを利用する端末のセキュリティ管理に関する事項（アカウントの登録並びにパスワード管理、OS等のセキュリティアップ デート並びにコンピュータウイルス対策など）

□ 本サービスを利用するアカウントの管理に関する事項（アカウント登録・削除、アカウント管理など）

□ 本サービスを利用して得られた情報の管理に関する事項（ダウンロードデータの保管・院外持出制限など）

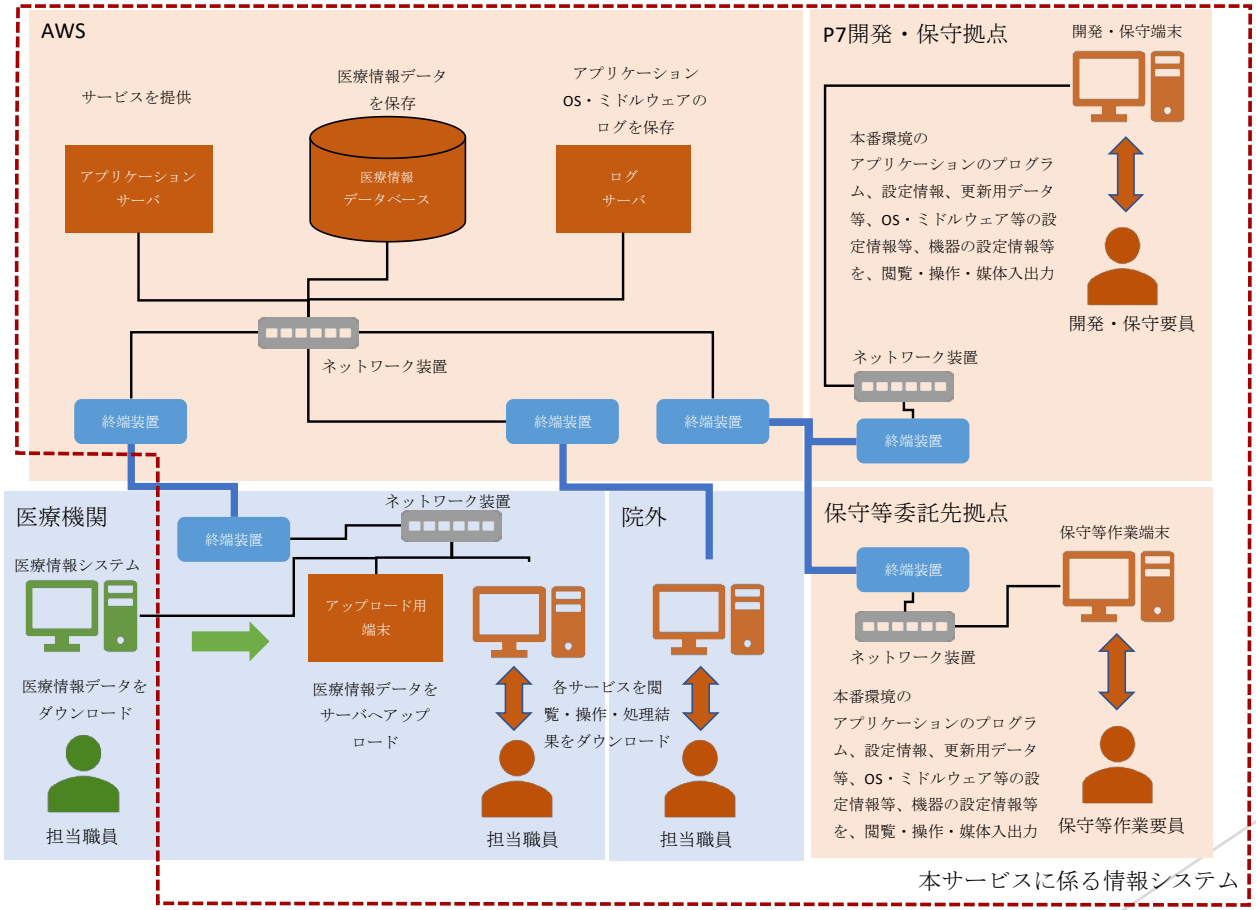
（２）医療情報 システムの安全管理に係る点検や評価の結果

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。

また、本サービスは医療 機関等の端末とはセキュリティを確保したVPN(Secure VPN Gateway) を利用した接続が限られたネットワーク接続で提供さ れており、リスクが顕在化する（攻撃が成立する）可能性は極めて低いと判断されます。

2. 医療機関等との共通理解を形成するために情報提供すべき内容

（３）医療情報システムの全体構成図



2. 医療機関等との共通理解を形成するために情報提供すべき内容

（４）リスク対応一覧

リスク対応								
対応するリスク		対応	対策の観点	対象事業社が実施する対策	医療機関へ対応を求める事項	残存リスク		
						影響度	顕在化率	リスク
受付/窓口の電子カルテ端末において	正当な者以外による医療情報の不正な閲覧や作成、更新が行われる	低減	人的・組織的対策	ー	医療機関等の職員への内部不正防止のための教育等は、医療機関等にて実施をお願いします。	ー			
			物理的対策	ー				
			技術的対策	端末のアプリケーション利用に際して、利用者を一意に識別するID/パスワード(8桁以上英数大文字小文字混合)による認証を実施する。				
	故意または過失による虚偽入力、書換により医療情報の改竄・破壊が行われる	低減	人的・組織的対策	誤操作防止のための医療機関等の利用者向けマニュアルを提供する。	医療機関等の職員への内部不正や誤操作防止のための教育等は、医療機関等にて実施をお願いします。	ー		
			物理的対策	ー				
			技術的対策	患者個人情報の更新や削除に係る履歴を、ログとして取得する。なお、法定保存期間が定められた情報に関しては当該期間の間ログを保存し、それ以外の情報については1年間ログを保存する。				
	アプリケーションに混入した脆弱性の悪用により、医療情報が見読不可となる	低減	人的・組織的対策	ー	ー	ー		
			物理的対策	ー				
			技術的対策	サーバ上で脆弱性スキャナーツールでの巡回を行う。				

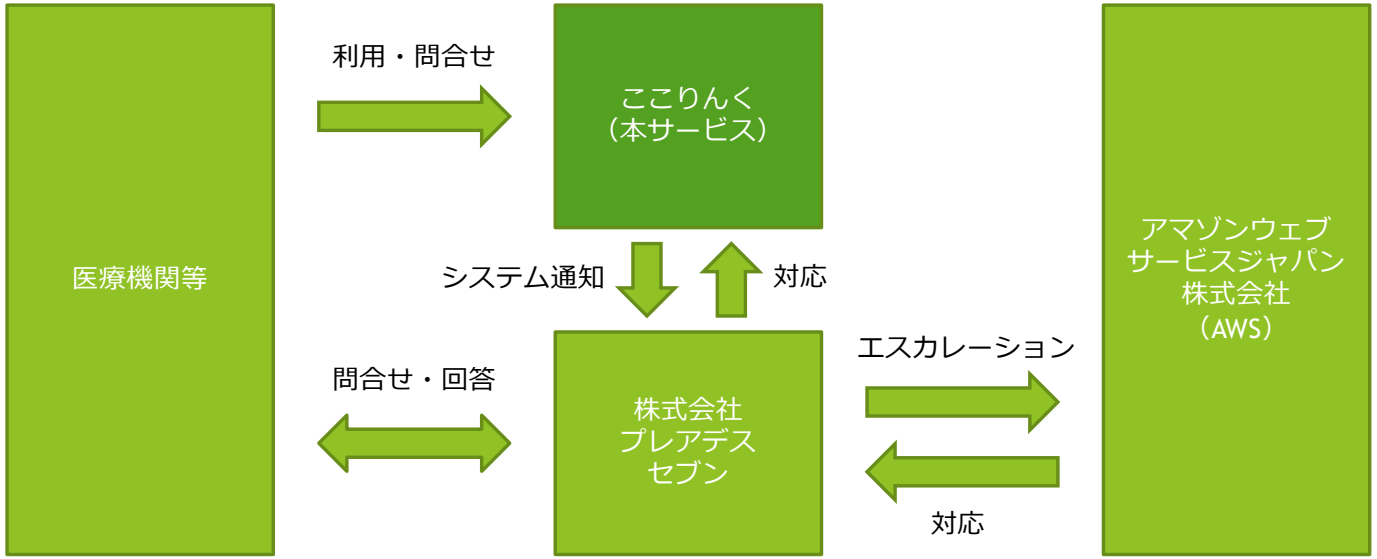
2. 医療機関等との共通理解を形成するために情報提供すべき内容

（ 5 ）医療情報 システムの安全管理に係る基本方針

個人情報のお取り扱いについて ：https://www.pleiades7.co.jp/privacypolicy/

2. 医療機関等との共通理解を形成するために情報提供すべき内容

（ 6 ）医療情報システムの提供に係る体制



2. 医療機関等との共通理解を形成するために情報提供すべき内容

（７）契約書・マニュアル等の文書の管理方法

契約書・マニュアル等の文書は、社内規定に則り管理します。

管理方法については、求めに応じて可能な範囲で開示します。

（８）機器等を用いる場合の機器等の管理方法

機器等については、運用手順書に則って管理します。

管理方法については、求めに応じて可能な範囲で開示します。

（９）リスク対応策の運用方法

運用手順書に則って、リスクの分析や必要な対応措置等を実施します。

運用方法については、求めに応じて可能な範囲で開示します。

（１０）事故発生時の対応方法及び医療機関等への報告方法

受託する医療情報が漏洩した場合には、速やかに、お客様管理者へご連絡いたします。

また、原因の究明、被害拡大の防止、その他お客様の情報の安全性の確保に必要な対応を行います。

なお、所管官庁その他関係機関への報告については、お客様管理者との協議により対応いたします。

2. 医療機関等との共通理解を形成するために情報提供すべき内容

（１１）医療情報 を格納す る記憶媒体の管理方法

医療情報は、「2.（３）医療情報シス テムの全体構成図 」にある AWS上に格納 し 、契約が継続する限り情報を蓄積し続けます。取外し可能な記憶媒体には保存いたしません。

また、サーバのHDD交換時には、AWS内で論理的または磁気的に破壊した後に廃棄いたします。

（１２）医療情報の外部保存に係 る患者等への説明方法

本サー ビスの利用に係る患者等への説明については 、第一次的には お客様において対応して頂くことと し 、当社においては 、必要な資料等 の提供等の範囲で対応させていただきます。

お客様において受託する情報を分析し、あるいは第三者に提供するために必要な加工を施す際に求められる患者等への説明と同意 に関しても同様といたします。

（１３）医療情報システムに対す る監査の実施方針

運用手順書に則って、定期的に情報 システム監査 を実施します 。

監査結果の概要については、求めに応じて可能な範囲で開示します。

（１４）医療機関等の管理者か らの問い合わせ窓口

※「2.（６） 医療情報システムの提供に係る体制」をご参照ください。

2. 医療機関等との共通理解を形成するために情報提供すべき内容

（１５）制度上の要求事項への対応

１） 医療分野の制度が求める安全管理の要求事項

☐ 個人情報の保護に関する法律、及び、同施行令並びに施行規則

☐ 個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・ 記録義務編、匿名加工情報編）、並びに、個人データの漏えい等の事案が発生した場合等の対応について

☐ 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

☐ 医療情報システムの安全管理に関するガイドライン 第5.2版（厚生労働省）

☐ 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（総務省・経済産業省）

２） 電子保存の要求事項

本サービスでは、e-文書法の対象範囲となる医療関係文書は取り扱っておりません

３） 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

本サービスでは、法令で定められた記名・押印を電子署名で行う文書は取り扱っておりません

４） その他取扱い注意を要する文書等の取扱い

本サービスでは、２）及び３）の他、取扱いに注意を要する文書等は取り扱っておりません

５） 外部保存の要求事項

医療情報の外部保存について、１）に記載の要求事項に準拠しております

改訂履歴

版数	発行日	改訂履歴
第1版	2023年2月28日	初版発行