



ResMed

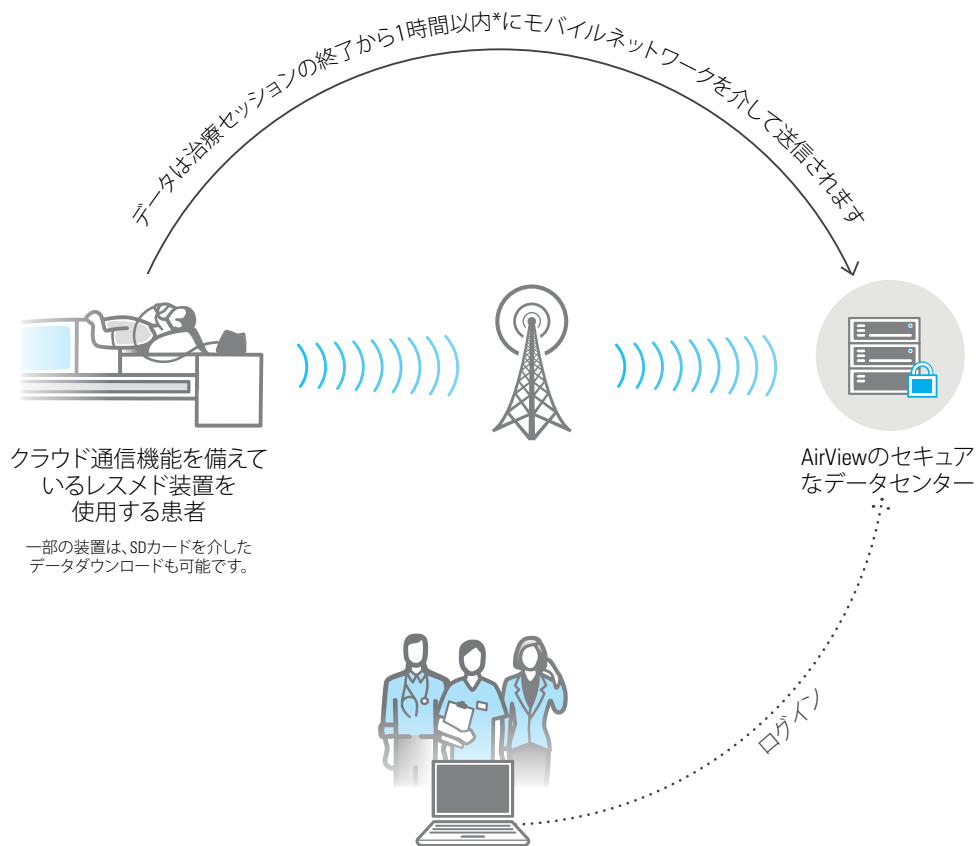
AirView™

Cloud-based patient management system

AirView™ データセキュリティ

AirViewは、睡眠時無呼吸症候群および呼吸不全の患者を管理するためのクラウド型ソリューションです。AirViewにより、医療従事者や担当の専門家は、診断から、装置のセットアップ、アドヒアランス、継続的管理まで、患者の各段階を容易に追跡することが可能になります。AirViewは、患者の転帰・予後と事業効率の向上をもたらします。

データフロー：
患者からAirViewを介して医療従事者および担当の専門家へ



- 装置データ送信
- 装置および患者データ送信

AirView ユーザー (たとえば、医療従事者および担当の専門家)
遠隔で患者の治療の状況を確認することができます。

*機種により所要時間は異なります。



AirViewは、信頼性の高いセキュリティ管理の元で個人情報保護の世界基準に準拠するように設計されています。レスメドは、初期設計から継続的モニタリングの運用まで、AirViewのすべての段階にセキュリティの専門家が関わっており、「プライバシー・バイ・デザイン」を実現しています。レスメド社内での取り組みに加え、外部の専門組織と協力して、技術および組織管理が実際に機能していることを定期的に確認しています。

構造

- AirView は、日本にある第三者施設管理のセキュアデータセンターでホスティングされています。
- このホスティング施設はISO27001認証取得の機構です。
- 高可用性でウォーム・フェイルオーバーの故障修復施設も日本に所在します。

データアクセス

- AirViewへのアクセス制限は、「知る必要性」原則に基づいています。
- AirViewは、物理的かつ、ネットワークレベルでもレスメド企業ドメインから分離されています。
- いずれのレベル(ネットワーク、サーバー、アプリケーション)でも、AirView へのアクセスは、レスメドのドメインへのアクセスとは分離されています。
- AirViewの管理タスクの実行権限は、レスメドIT担当者の一部に限定されます。
- AirViewにアクセスするレスメドの社員は、毎年個人情報保護の研修を受講しています。
- AirViewを扱う組織は、いずれも、アプリケーション内の特定の役割をどの社員が行うかを決めています。
- メニューオプションとワークフローは、あらかじめ決められた役割によって変わります。この役割によって、組織の方針や基準に合うように職掌分散を実施することができます。
- パスワードの複雑性が強化されており、組織はパスワードの有効期限を組織の方針に合うように選択できます。

データの暗号化

- AirView は、データベース暗号化技術を使用し、患者データをセキュアに保ちます。
- AES 暗号化アルゴリズムでは256ビットの変調長さが使用されています。
- AirView とのすべての通信は、SSLおよびhttpsテクノロジーを使って暗号化されます。
- すべてのテープバックアップは、変調長さ256ビットのAESを使って暗号化されます。この暗号化は、バックアップ基盤において実施されます。

リスク管理および個人情報保護コンプライアンス

- レスメドは、広く使用されている脆弱性スキャンツールを使用して、AirViewの基盤およびアプリケーションに脆弱性が見られないか定期的に検査しています。スキャン結果については再調査を行い、適切な是正措置を実施します。
- 大手の専門セキュリティ会社がAirViewの基盤レベルおよびアプリケーションレベルで侵入テストを実施します。
- レスメドは、ビッグ4の監査法人による外部監査を受け、SOC-2およびAT 101証明を付与されています。AT 101 証明は、米国NIST 800-66 HIPAA コンプライアンスガイドをフレームワークとして使用し実施されました。

経験を積み、訓練を受けた、有資格のセキュリティチーム

- レスメドでは、情報セキュリティとコンプライアンスの分野で経験を積んだ多様なセキュリティチームが活躍しています。
- チームは、CISSP、CISM、CISA、CRISC、MRMIA、CEH、CCNAを始めとする世界的なセキュリティおよび技術認定を取得しています。

監査統制

- AirViewのセキュリティおよび監査ログは、疑わしい違法行為がないかどうか、日常的に監視されています。

注記:保護されたい医療情報は、このログには保存されません。