**ResMed**

AirView™
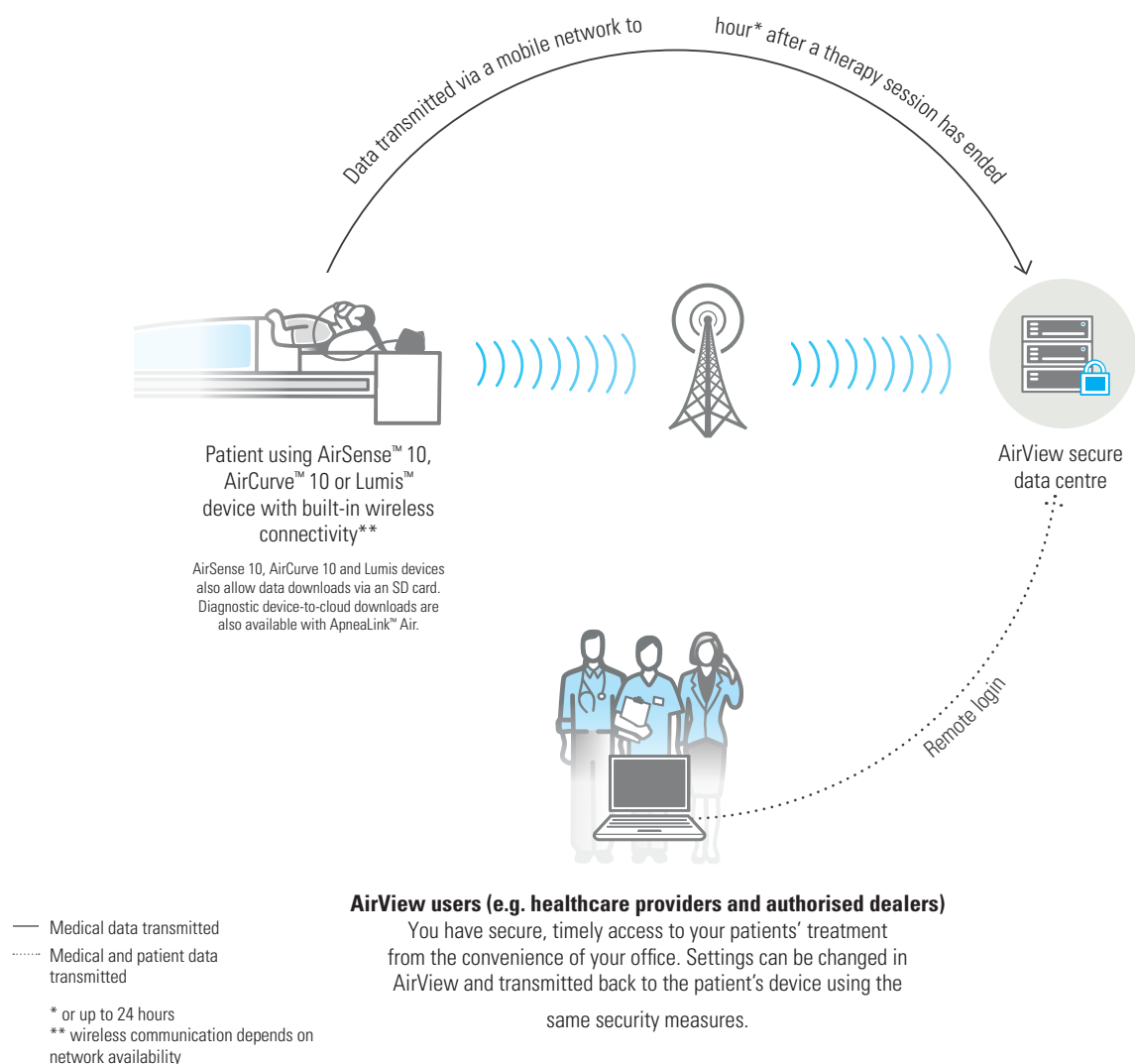Cloud-based patient management system

# AirView™ data security

AirView is a cloud-based solution for managing patients with sleep apnoea and respiratory insufficiency. AirView makes it easy for healthcare providers and authorised dealers to follow each patient's journey from diagnosis, through to equipment setup, adherence, and ongoing monitoring. AirView is part of ResMed Air Solutions, and helps to improve patient outcomes and business efficiencies.

The flow of data:
from patients to AirView to healthcare providers and accredited partners

Data transmitted via a mobile network to hour* after a therapy session has ended

Patient using AirSense™ 10, AirCurve™ 10 or Lumis™ device with built-in wireless connectivity**

AirSense 10, AirCurve 10 and Lumis devices also allow data downloads via an SD card. Diagnostic device-to-cloud downloads are also available with ApneaLink™ Air.

AirView secure data centre

Remote login

**AirView users (e.g. healthcare providers and authorised dealers)**
You have secure, timely access to your patients' treatment from the convenience of your office. Settings can be changed in AirView and transmitted back to the patient's device using the same security measures.

— Medical data transmitted
···· Medical and patient data transmitted

* or up to 24 hours
** wireless communication depends on network availability

ResMed.com/AirSolutions

AirView was built from the ground up to be secure and compliant with global privacy legislations. In Australia, AirView is compliant with the Australian Privacy Act 1988, including the new 2014 Australian Privacy Principles. ResMed performs Privacy by Design, ensuring that security specialists participate in all steps of AirView, from the initial design to perpetual monitoring of operations. In addition to ResMed's activity, we regularly engage with external specialist organisations to validate that the technical and organisational controls are operating effectively.

## Infrastructure

- AirView is hosted in a secure data centre located in Japan provided by a third party service provider.
- The high availability and warm-failover disaster recovery site is also located in Japan.
- The hosting service provider has current ISO27001 certificates.

## Data access

- Restricted access to AirView is based on the 'need to know' principle.
- The ResMed data centre limits access to authorised personnel only, and is secured by a locked door.
- Individual server racks located within cages are also fitted with a door-locking mechanism.
- AirView is isolated from the ResMed corporate domain at the logical level, and also at the virtual network level.
- Access to AirView at any level (network, servers, application) is separate from access to the ResMed domain.
- Only a subset of ResMed IT personnel is authorised to perform administrative tasks for AirView.
- ResMed employees who access AirView undergo annual privacy training.
- Each organisation using AirView determines which employees perform specific roles in the application.
- Menu options and workflows will vary based on predefined roles. The roles allow organisations to enforce a separation of duties to fit their policies and standards.
- Password complexity is enforced, and organisations can select the password ageing frequency that matches their organisation's policies.

## Data encryption

- AirView uses database encryption technologies to secure patient data.
- The AES encryption algorithm is used with 256-bit key length.
- Backup keys are stored in a secured and monitored location separate from the data.
- All communication with AirView is encrypted using SSL and https technologies.
- All tape backups are encrypted using AES with 256-bit key length. This encryption is performed within the backup infrastructure.

## Risk management and privacy compliance

- ResMed uses a market-leading vulnerability scanning tool to regularly assess the AirView infrastructure and application for vulnerabilities. Results of the scans are reviewed and appropriate remediation is performed.
- AirView has been penetration-tested at the infrastructure and application levels by a leading specialist security firm.
- ResMed has undergone an external audit from a leading Big Four accounting firm to provide a SOC-2 and an AT 101 attestation. The AT 101 attestation was performed using the US government NIST 800-66 HIPAA compliance guide as the framework.

## Experienced, trained and certified security team

- ResMed employs a diverse security team with over 80 years of combined experience in information security and compliance.
- The team holds global security and technical certifications such as CISSP, CISM, CISA, CRISC, MRMIA, CEH, CCNA and others.

## Audit controls

- The security and audit logs of AirView are regularly monitored for suspicious and actionable activity.

  **Note:** No protected health information is captured in this logging.

ResMed.com/AirSolutions