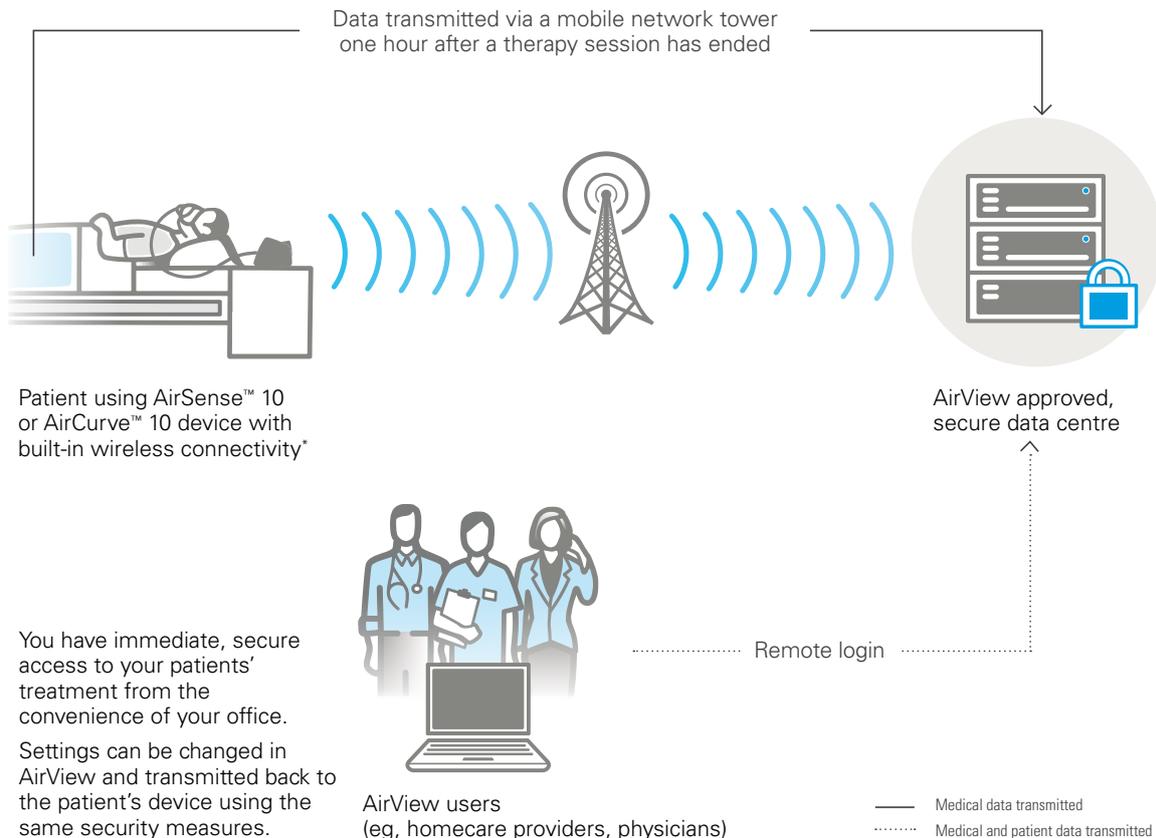# AirView data security

AirView is a cloud-based solution for managing patients with sleep and respiratory insufficiency. AirView makes it easy for physicians and healthcare professionals to follow their patients' journey from diagnosis, through to equipment set-up, compliance, and remote monitoring. AirView is part of the new ResMed Air Solutions, and helps to improve patient outcomes and business efficiencies.

The flow of data:
From patients to AirView to healthcare professionals

Data transmitted via a mobile network tower one hour after a therapy session has ended

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

AirView approved, secure data centre

You have immediate, secure 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.

AirView users
(eg, homecare providers, physicians)

Remote login

——— Medical data transmitted

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

Card-to-cloud option

AirSense 10 and AirCurve 10 devices also allow data downloads via an SD card**

* AirView also works with ResMed's S9™ device series with wireless module attached. Data is transmitted from S9 devices daily, at a fixed time.
** Diagnostic device-to-cloud downloads are also available with ApneaLink™ Air.

ResMed.com/AirSolutions
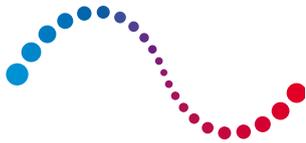
ResMed

AirView was built from the ground up to be secure and compliant with EU 95/46/EC and national privacy law. The ResMed security team participated in every step involved in creating, launching and managing AirView: requirements, design, development, testing, deployment and operations. Multiple external specialist organisations (such as, Boulder CO) have tested and assessed AirView for the technical and organizational controls necessary for French ASIP compliance.

Infrastructure

- AirView is hosted by IDS: a third party company that holds the French ASIP Santé certification to host medical data, ensuring high security standards.
- IDS operates two data centres both located in France. The primary system is located in Montceau les Mines; the backup system in le Creusot. The two centres are connected through a dedicated 10 Gb optical fibre.
- Both primary and backup centres have dedicated external networks with failover, which guarantees a high level of access.

Data encryption

- AirView uses database encryption technologies to secure your data.
- The AES encryption algorithm is used with 256-bit key length.
- All communication with AirView is encrypted using SSL and https technologies.
- All tape backups are encrypted using AES with 256-bit key length in a the backup data centre located at Le Creusot (France).

Data access

- Only authorised IT personnel can perform administrative tasks for AirView.
- All database accesses are logged and can be retraced.
- Each organisation using AirView determines which employees perform specific roles in the application.
- Users who want to gain access to AirView need to have an account created for them by the organisation's administrator, and install a certificate provided by the IDS.
- The certificate only provides access with one PC and one browser. If several PCs need to be used, multiple certificates need to be installed.
- Menu options and workflows will vary based on predefined roles. The roles allow organisations to enforce 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

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.