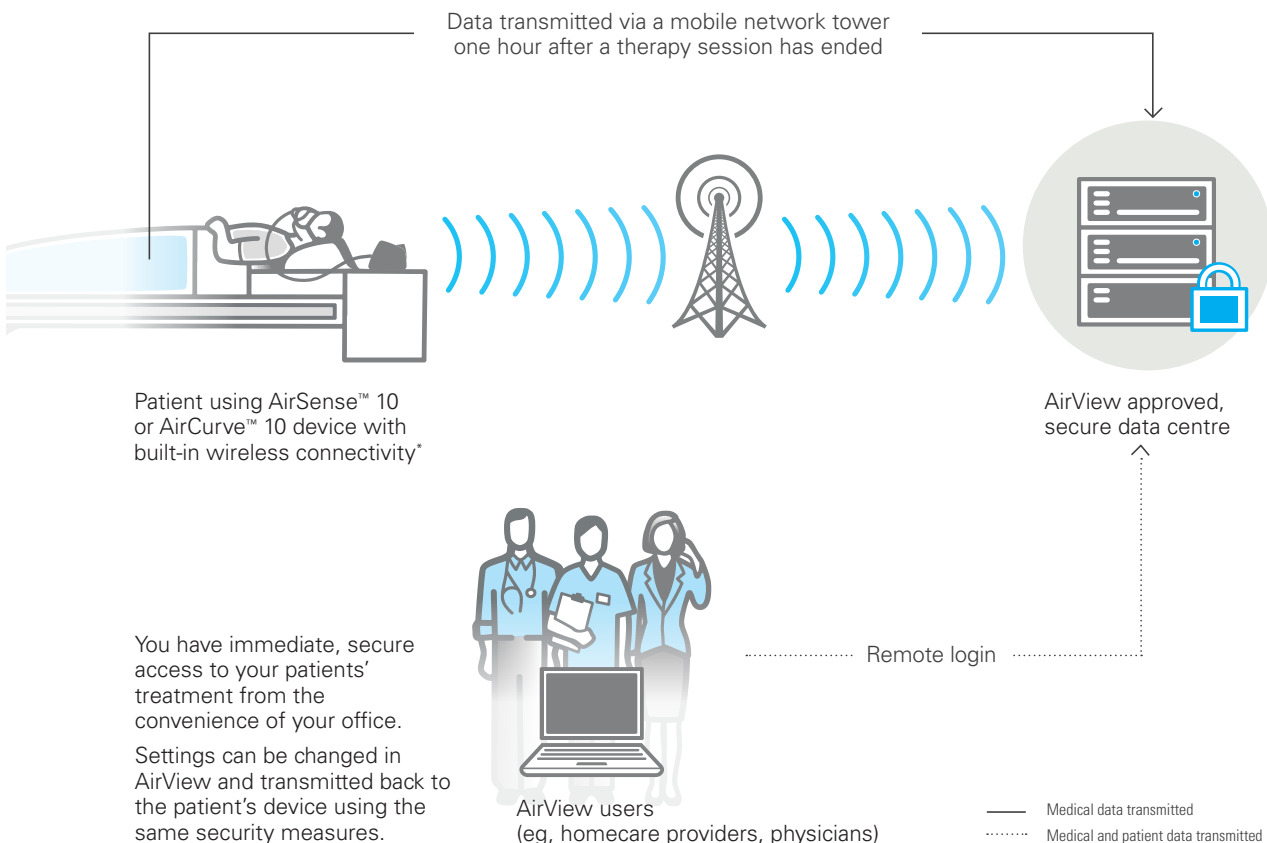


# AirView data security

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

The flow of data:  
from patients, to AirView, to healthcare professionals



## 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.



AirView was built from the ground up to be secure and compliant with EU 95/46/EC and national privacy law. 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 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 the backup data centre located at Le Creusot.

### 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 the separation of duties to fit their policies and standards.
- Password complexity is enforced, and organisations can select the password ageing frequency that matches their 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.



**ResMed Ltd**  
1 Elizabeth Macarthur Drive  
Bella Vista NSW 2153 Australia

**DISTRIBUTED BY**  
**IEC/REP** ResMed (UK) Ltd 96 Jubilee Avenue  
Milton Park Abingdon Oxfordshire OX14 4RW UK

See [www.ResMed.com](http://www.ResMed.com) for ResMed locations worldwide. AirCurve, AirSense, AirView and S9 are trademarks of ResMed Ltd. ApneaLink is a trademark of ResMed R&D Germany GmbH. S9 and ApneaLink are registered in the U.S. Patent and Trademark Office. Specifications may change without notice. ©2014 ResMed Ltd. 1017596/1 2014-07

