Privacy and security

Involve Interpreter powered by Attend Anywhere | Last updated: Apr 03, 2020

Read more about the steps Attend Anywhere takes to ensure video consultations are safe, secure, and private.

What are the differences between security, privacy, and data sovereignty?

- **PRIVACY** relates to the appropriate use of collected information, as required by the Australian Privacy Act 1988, and the Australian Privacy Principles.
- **SECURITY** ensures that both video calls and related information systems are safe from unauthorised access and use, ensuring that the data is reliable, accurate, and available for use when needed.
- **DATA SOVEREIGNTY** means that patient information and data must stay within territorial boundaries required by Privacy Legislation (or be covered by accredited data protection equivalence)

Management console privacy and security

Health-grade privacy, security, and data protection are fundamental to Attend Anywhere's design. The Management Console and its network architecture are covered by design assurance processes to ensure that new features and capabilities continue to meet the required standards.

Security

While WebRTC video call media traffic is protected with AES 256-bit encryption between web browsers, expecting this to be adequate protection in the patient health-care setting would be naive. For example, call encryption does not help if someone is able to highjack the signalling and listen in on the call.

As the volume of video consultations grow, there is a heightened public awareness around privacy and security, and the measures taken to protect against:

- Someone impersonating a clinician. *Example: Gaining access to the video room.*
- Unauthorised observation of a consultation. *Example: Gaining unauthorised access ('hacking') the video call signalling.*
- Third parties accessing the history of a consultation. *Example: Observing the call logs on the patient device).*

Unlike provider-centric meetings, video chat, or conferencing based architectures (which are inherently less private and secure), Attend Anywhere has a **three-tier privacy and security model** that involves:

- Ensuring access is via a single point on the service provider website.
- Creating private video rooms for each consultation.
- Ensuring that the media signalling cannot be hacked in order to impersonate a clinician, or observe a consult. (Not simply protecting the call content.)
- Ensuring only authorised service providers from the clinic can join patients' rooms.
- Ensuring the media content is secure.

Privacy

The Management Console is compliant with government privacy policies in Australia and the UK.

The Management Console is implemented and run according to a System Security Policy approved by NHS National Services Scotland. This incorporates GDPR- and UK Data Protection Act 2018-compliant controls and policies.

Patients enter online Waiting Areas via a trusted service provider website and wait in their own private video room. It doesn't matter if a Service Provider is running overtime with another patient, as there is no chance of people running into each other. The room is deleted after the consultation.

Patients can be seen by any Service Provider authorised to access the Waiting Area. Authorisation is defined by a unique login and assigned roles in the platform. Organisation Administrators are responsible for assigning this access to their staff.

The Management Console does not retain patient-identifiable information which means patients using the Attend Anywhere service leave no digital footprint.

Attend Anywhere's hosting practices

Attend Anywhere's hosting is operated under an extensive range of security measures, components, and controls, which deliver a robust and secure environment for digital health services.

The Attend Anywhere Management Console and its network architecture are covered by design assurance processes, to ensure that new features and capabilities continue to meet the required standards.

Data Sovereignty

All call records and related provider data within the Attend Anywhere Management Console, stay within sovereign territorial boundaries as required by Privacy Legislation in the UK and Australia.

Infrastructure and application protection

The Attend Anywhere Management Console hosting and web application has multiple layers of protection from web attacks and exploits.

- Web Application Firewall (WAF) with comprehensive Open Web Application Security Project (OWASP) Top 10 coverage
- Distributed Denial-of-Service (DDoS) protection
- Application server systems protection covering:
- Malware and virus protection
- Automated system vulnerability assessment
- On host intrusion protection and detection system
- Virtual patching providing automatic update of protection modules for newly discovered vulnerabilities even before operating system or vendor patches are available.

Infrastructure and application testing

- Attend Anywhere, as part of infrastructure and application assurance, maintains a suite of standard security testing tools
- Regular external-facing testing is performed to ensure infrastructure attack surface-area complies with the design and deployment specifications
- Server configuration and software versions are audited against currently-known vulnerabilities
- The application hosting environment is audited for any inadvertent misconfiguration
- Third-party-contracted testing is performed in concert with key stakeholders

Hosting

- The system is provided as resilient, high availability, hosted service
- Underlying infrastructure is provided by accredited cloud providers, with redundant and resilient internet connections and local utilities
- All systems are hardened according to recognised standards

- All data transported between users and all system components is encrypted
- All data at rest is encrypted

High availability

The system is designed for continuity with resilience to site and component failures.

- Redundant sets of components are deployed into geographically-separated sites. These redundant components are configured for cross-communication, so that if a component fails in a given zone, its functions will be fulfilled by surviving components in the alternate site.
- The design is scalable with additional component units able to be added for resiliency, and capacity.