We're serious about security

We know that your personal information, as well as the healthcare information shared in our network, is some of the most sensitive data around. That's why everything we do is underpinned by best-in-class security and data privacy compliance.

Accredited and compliant for healthcare

- General Data Protection Regulation
- ISO 27001 Certified Data Centre
- SOC2 Certifed MS Azure Cloud
- Cyber Essentials
- Information Commissioner's Office
- UK G-Cloud 12 Certified Provider
- IRAP Certifed MS Azure Cloud
- Compliant with OAIC Privacy Act
- NSW Govt. Certified Provider
- Department of Internal Affairs Marketplace
- Health Information Standards Organisation
- NHS DSP Toolkit & Information Governance
- Organisation for the Review of Care & Health Applications

Patient Comes First

With Celo the Patient's privacy comes first. All communication and information related to a patient is securely stored on our encrypted database. No patient information is stored permanently on a Celo user's device, including any clinical photographs captured.

Celo is compliant with regional requirements. See our compliance section for more information.

Authenticated Healthcare Network

Celo features an Authenticated Healthcare Network. By authenticating all users of Celo, we ensure an up to date and safe network of healthcare professionals. Using Celo, finding the right colleague at the right time is easy and secure.

Active Directory integration is available for our Enterprise customers.

Join Celo at
www.celohealth.com

Mobile Device Security

Access Celo securely by using biometrics or your Celo PIN number. No patient information is stored permanently on a Celo user's device, including any clinical photographs captured. All patient information is securely stored on the server. This ensures that if a user loses their device, that patient information is not compromised.

Secure Clinical Photos

All photos in Celo are captured from inside the Celo App. All photos are watermarked with patient and Celo user information as well as a timestamp, and uploaded to the server as soon as they are taken. Celo photos are not stored on the local camera roll and are instead securely stored on the server.

Communication Security

When a healthcare professional on the Celo network accesses patient information through the app it is sent over a secure channel (2048 bits HTTPS using sha256RSA) and only stores the information in the phone's memory while the app is active, after which it is automatically removed.

Secure 3rd party integration

Celo integrates with Electronic Medical Records. This improves patient safety and allows auditing. Integration via RESTful APIs with multi factors of authentications like API Keys, (Mutual SSL), IP restrictions and more. Ensure clinical images or important notes are filed to patient records appropriately. We support HL7 or FHIR integration.

HL7 FHIR

Join Celo at
www.celohealth.com

celo

Compliance

To protect patient health information and Celo user information as required by many privacy laws around the world, Celo's databases use the most thoroughly compliant cloud service provider to store and process all data. Microsoft Azure has more certifications than any other cloud provider and is compliant with many international, industry-specific and country-specific standards. These standards include General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, Australia IRAP, UK G-Cloud, NZ HISO and Singapore MTCS. Microsoft Azure is also rigorously audited by third party authorities such as the British Standards Institute to ensure all standards are met.

Celo takes the security of patient information very seriously, which is why we work with a Crest Accredited security partner for a wide range of security testing. Ongoing security testing includes source code reviews and penetration testing. Additionally, Celo strives to be even more secure than required standards, by working with regulators to seek approval from national and government health organisations; allowing organisations to run their own technical analysis on the Celo platform, and protecting all data with each individual Celo user's unique password and passcode. Globally, Celo works closely with large health providers and government to continually improve our service and remain compliant.

Safe Storage of Patient Data

We use Microsoft Azure cloud storage and our data centres are located around the world for our different customers. Celo is compliant with regional requirements. See our compliance section for more information.

Our Azure databases use Transparent data encryption (TDE) to help protect data against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest.

On top of this, fields containing patient data are encrypted using AES-256.

Celo's databases utilise Microsoft Azure's active geo-replication enabling secondary databases in different locations (regions), allowing for failover if there is a data centre outage or the inability to connect to the primary database.

Raw access to Celo's database servers requires multiple levels of authentication and Celo's technical staff working on the servers must undergo mandatory police and background vetting checks.