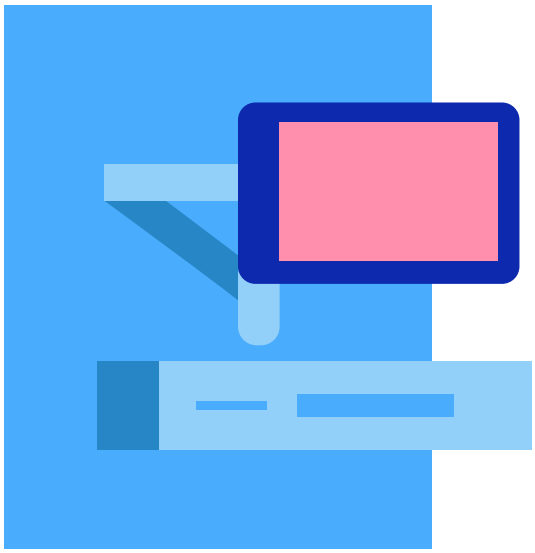
celo

Cloud Policy



Celo Cloud Policy

Summary

- Celo is a secure and healthcare compliant alternative to using texting, email and consumer apps such as WhatsApp to send patient information.
- Celo is a platform which has been built using healthcare industry best practice security guidelines, data encryption during transfer and at rest as well as a range of other security measures as outlined in this document.
- Celo uses Microsoft Azure cloud storage and data centres which are located around the world for our different customers. Celo is compliant with regional requirements. See our Legal Section for more information.
- Microsoft Azure is a healthcare compliant environment.
- By accepting the Celo Terms and Conditions of Use, healthcare providers can join a compliant and safe network to communicate patient information and ensure they look after their patient's health information.

Healthcare Compliant Platform

Celo is a secure communication, collaboration, and community platform created specifically for people in healthcare, by people in healthcare.

Celo ensures patient information is kept safe and secure, improves workflow and delivers patient care more efficiently, while always keeping the patient first in mind and at the centre of care.

What rights do individuals have over their personal data?

- The Right of Access
- The Right to Erasure
- The Right to Rectification
- The Right to Restriction
- The Right to Objection
- The Right to Portability
- The Right to Complain

Please see our Privacy Policy for more information about these rights.

Data Sovereignty and Localisation

Celo User Data and User Generated Data are stored as outlined in the tables below:

Data Subjects	Data Categories
Celo User Data	Name, address, telephone, email, usernames, GMC or health profession registration number, proof of identification for validation (passport or driving licence)
User Generated Data	Message data, images, Patient ID, Date of Birth, Gender, Name, Health Information, and/or other data as generated by a Celo user

Celo User Region	Celo User Data Location	User Generated Data Location
European Union	Replicated across the following data centres: • North Europe (Ireland) • Australia	North Europe (Ireland)
United Kingdom	Replicated across the following data centres: • North Europe (Ireland) • Australia	North Europe (Ireland)
Australia	Replicated across the following data centres: • North Europe (Ireland) • Australia	Australia
New Zealand	Replicated across the following data centres: • North Europe (Ireland) • Australia	Australia

Celo Platform

The Celo Platform, accessed through a mobile app installed on a mobile device or via the desktop app, provides a secure communication, collaboration, and community platform

Celo's main functionality is described below:

1. Real-time communication between clinicians by way of instant messaging.
2. Capturing patient images for sharing with colleagues which are stored securely.
3. Networking with other verified health providers to quickly connect and discuss patient cases.
4. A patient consent process for the capturing of images which is described further below.

Patient Information

Patient information will primarily be images of the patient anatomy and messages related to the patients care and treatment. The information will include patient ID numbers and other identifiers including: first name, last name, DOB and Gender. Patient information is included under the "User Generated Data" category as described earlier in this document.

Celo and the NHS Digital DSP Toolkit

Celo is compliant with NHS Digital's DSP Toolkit. You can look us up on the NHS DSP Toolkit website by our name or registration code: YGMYJ. The DSP toolkit allows Celo to ensure that our Data security and Protection practices conform to the National Data Guardian's 10 data security standards. These standards and other information can be found here. The toolkit is updated frequently and must be completed by all organisations that have access to NHS patient data and systems to ensure that all organisations are practicing best practice data security and sensitive information is being handled correctly.

Privacy and Confidentiality

1. Login

The app must be accessed only by the health provider logging in with their unique login, I.e. Secure access. This enables the health provider to commence messaging and also gives them access to stored images/messaging where they have either been the sender or the recipient of that information. The health provider cannot access other information stored for patients whose care they have not been involved in.

2. Patient consent

The application contains an optional digital consent process that has been developed with input from large clinical organisations. The optional digital consent process ensures that patient consent can be easily obtained when required for taking and use of clinical images.

3. Transfer of data

Data is automatically encrypted throughout the entire lifecycle during transfer and at rest. All database backups are encrypted as well.

4. Storage of data

No patient information (including images and consents) is permanently stored on the mobile device from which the information was sent or received. All patient information is stored in a Microsoft Azure cloud environment as per our localisation table outlined earlier in this document. Celo also utilises Microsoft App services. It is also worth noting that Microsoft spends over $1 billion on cybersecurity per annum.

Privacy policy and terms and conditions

Celo will notify all users when any updates or amendments are made to our Privacy Policy or Terms and Conditions of Use. It is the Celo User's responsibility to update their own policies to reflect these if any changes affect patients and patient details.

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.

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 the compliance section on our website 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.

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

All photos in Celo are captured from 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 Third-Party Integration

All photos in Celo are captured from Celo integrates with Electronic Medical Records. This improves patient safety and allows auditing. Integration vis 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.

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.

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.

Messaging in the Healthcare Workplace

In the healthcare sector, there are mobile devices everywhere which are often being used at the point of care. In particular, clinicians at hospitals and healthcare organisations are using consumer text-messaging and instant-messaging apps to communicate and discuss patient details due to the convenience of these services. This can violate health privacy standards, including HIPAA (USA), GDPR (EU & UK), HISO Regulations (NZ), or OAIC (AUS) regulations. At Celo, we have solved the problems this presents and have become an integral part of the healthcare sector by offering compliant and secure solutions to individuals and organisations.

Evidence from the British Medical Journal

A recent study published in the British Medical Journal: "The ownership and clinical use of smartphones by doctors and nurses in the UK", found that:

- 98.9% of clinicians own a smartphone
- over 90% of clinicians use a healthcare centred app

However, a survey published in the Journal of Hospital Medicine reported that:

- 27% of clinicians use a secure messaging application in the workplace
- only 7% said most clinicians were using a hospital-issued messaging app

While almost all clinicians have access to a smartphone, a majority were wrongfully using consumer applications readily available to non-healthcare professionals.

An article published in the British Medical Journal titled *"Wanted: a WhatsApp Alternative for Clinicians"* shows that WhatsApp is a valuable tool in the healthcare sector, even if it does not comply with health privacy laws such as the GDPR.

The article showed that the huge risks of using WhatsApp in a clinical setting are outweighed by the benefits. This highlights a problem in the healthcare sector that needs to be solved quickly as over 90% of clinicians are already using their smartphones in the workplace. The NHS England states that "WhatsApp should not be used for clinical communications".

Celo solves healthcare privacy risks

Authenticated

Celo verifies users by identity and profession, so you can make sure you are talking to the right person. Celo also verifies healthcare organisations. The Celo app is always pin code or biometrics protected.

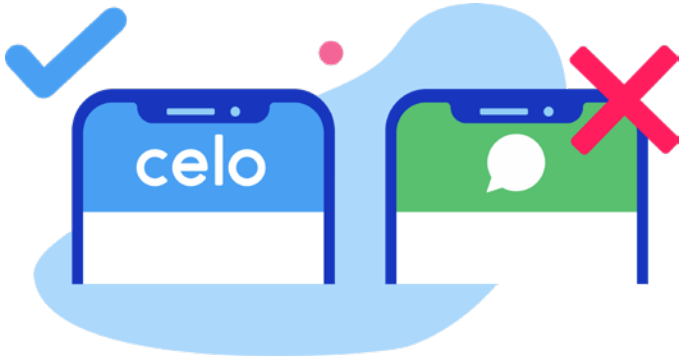
Secure

All Celo data is stored securely on Celo's compliant servers, which are healthcare grade encrypted, in your Celo secure library. No patient information is stored permanently on a Celo user's device, including any clinical photographs captured.

Encrypted

All data is stored in a regionally and healthcare compliant Microsoft Azure Data Centre that is compliant with ISO 27001, GDPR, HIPAA, HISO regulations and OAIC regulations. All data used by the Celo app and end user is also encrypted using sha256RSA.

Why is WhatsApp not compliant for medical use?



- Data and photos are stored on your personal device.
- The servers, owned by Facebook, are based in the US.
- WhatsApp is not pin protected.
- You require personal phone numbers to message individuals.
- Easily mixed with personal contacts and communications.

Issues with using non healthcare specific messaging applications

The research from the British Medical Journal and the Journal of Hospital medicine reveals a clear demand from clinicians for Celo, and the integration of mobile technology into healthcare workflows. While services like WhatsApp are easily accessible, they come with a number of risks, including:

Lack of security and encryption

- Consumer messaging applications are built for communication between friends, but they should never be used for sharing confidential information.
- Apps like WhatsApp are end-to-end encrypted. However, these apps usually are not password protected and store data on the local device storage which is accessible if somebody steals or finds a lost device.
- If a phone is lost or compromised, an unauthorised individual would have access to every message and photo.
- Anybody can download messaging apps from the app store and sign up to them. This means sensitive information could be accidentally sent to a member of the public.

Not auditable

- Consumer messaging apps cannot be audited by a higher authority. E.g Enterprise providing the service to their employees
- Consumer messaging apps do not follow data sovereignty and localisation laws or policies that most health authorities require.
- Many conversations about an individual's medical information need to be stored within electronic health records. (Records allow clinicians, who haven't previously been included in conversations, to see developments and the latest updates).
- Messages on consumer apps can simply be deleted, making any record of what was sent and received difficult to trace.

Photo syncing

- Taking a photo on a smartphone is a convenient way for a clinician to show, document, and share patient information.
- Many smartphone systems automatically sync photos to cloud services. This auto-backup function poses a security threat for clinicians, especially if the cloud photo account is shared with family members or the public.
- Smartphones store photos in an unencrypted state. If access was gained to a clinician's phone by an external party, sensitive patient photos could be accessed with relative ease.
- Patient consent is needed for clinical photography; consumer grade messaging apps do not have a facility to show that consent was given for a clinical photograph to be taken.

Data mining

- While data is usually secure and encrypted, it is not always private.
- Patient information may be falling into the wrong hands through no criminal or negligent use by clinicians, by simply not knowing the app they are using lacks security by design.

Celo Presents:

A Secure and Encrypted App

All Celo data is password protected and encrypted with healthcare grade protocols. No patient information is stored permanently on a Celo user's device, including any clinical photographs captured. As such, Celo cannot be compromised if unauthorised access is gained to your phone. Celo verifies users by identity and profession, so you can make sure you are talking to the right person.

Auditability

Celo data is securely stored and can be integrated to Electronic Medical Records. Furthermore, Celo data is stored to be compliant with data sovereignty requirements.

Celo Secure Library

Photos and documents stored or created in Celo are only saved to the Celo Secure Library and not saved on the user's device. The Celo Secure Library is not synced with any third party servers or cloud services. Celo allows clinicians to optionally attach a record of consent to all clinical photos.

Privacy by Design

Data in your Celo Secure Library is private unless you choose to share it with a healthcare professional from the Celo Verified Network.

Conclusion

There are numerous benefits to using mobile communication apps within a healthcare organisation. However, there needs to be an emphasis on:

- The use of healthcare centred messaging apps.
- The protection of patient data.
- Adherence to strict organisational policies to stay compliant with the law.

With Celo, clinicians can have the convenience of texting without putting private patient information at risk, and healthcare organisations and authorities can support them in doing so, ensuring they won't turn to the App Store for less-than-ideal solutions.