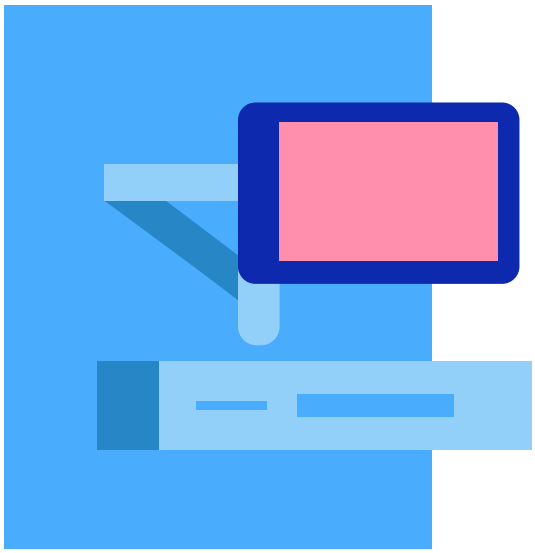
celo

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 centers which are located around the world for our different customers. Celo is globally accredited and compliant for healthcare. 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 utilizes the cloud to deliver its services. Celo User Data and User Generated Data is stored as outlined in the tables below:

Data Subjects	Data Categories	Data Location
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	Dependent on Celo User Country as per the below table "Celo Cloud Storage Location - User Generated Data"
Celo User Data	Name, address, telephone, email, usernames, GMC or health profession registration number, proof of identification for validation (passport or driving licence)	Replicated across the following data centres: • North Europe (Ireland) • Australia

Celo Cloud Storage Location - User Generated Data

Celo User Country	User Generated Data - Cloud Storage Location
United Kingdom, Ireland, United States, Switzerland, South Africa, Senegal, Zimbabwe, Zambia, Kenya, Nigeria, Tanzania, Pakistan, All other countries	North Europe (Ireland)
New Zealand, 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.

Patient Information

Patient information will primarily be images of the patient anatomy and messages related to the patient's 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 organizations that have access to NHS patient data and systems to ensure that all organizations are practicing best practice data security and sensitive information is being handled correctly.

Celo and HIPAA

Specifically related to HIPAA, the Celo platform enables our users to Use (share within their healthcare organization) or Disclose (share with another healthcare organization) patient data as allowed by the US HIPAA Regulations. Under the HIPAA Privacy Rule, Protected Health Information (PHI) may be Used or Disclosed for treatment, payment or healthcare operations without patient consent. Uses and Disclosures must follow the HIPAA regulations, including the Minimum Necessary rule, and must comply with the policies and procedures of the Celo user's organization.

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.