Celo

Celo Cloud Policy

New Zealand

Celo Microsoft

Celo hiso Microsoft ISO AICPA SOC 2

Celo Cloud Policy
New Zealand

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 including HISO (Health Information Standard Organisation), 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 which is hosted in Australia data centres.
- Microsoft Azure is a healthcare compliant environment.
- In accordance with New Zealand privacy law, and in guidance with the Ministry of Health, users of Celo within New Zealand must complete a Cloud Risk Assessment to use the Celo service.
- Celo has completed a detailed Cloud Risk Assessment on behalf of our Celo users (outlined here).
- By accepting the Celo Terms and Conditions and Cloud Risk Assessment, healthcare professionals can join a compliant and safe network to communicate patient information and ensure they look after their patients health information.

Celo Cloud Risk Assessment

This risk assessment can be adopted by healthcare professionals that wish to use Celo's secure messaging services. This is required as the information created in Celo utilises offshore (Australian) data centers managed by Microsoft. This process is a requirement under New Zealand privacy law as detailed by the Ministry of Health. It is also worth noting that Microsoft spend $1 billion annually on cyber security and do not have data centers located in New Zealand. No provider in New Zealand at this time can match Microsoft's level of data security investment.

For large healthcare organisations such as District Health Boards, this risk assessment can also be adopted or an independent risk assessment can be carried out. Celo has undertaken the GCIO cloud computing questionnaire for several of our enterprise customers and this is available to our customers upon request.

Background

Clinicians often seek input from colleague's who are offsite/not in the immediate vicinity. This can involve patient images being taken on a mobile device and sent to another (often more senior) clinician for their input. The process is not particularly secure, and the information captured is retained in the sender and receivers mobile devices and as such becomes subject to all the rules relating to 'health information' set out in the Health Information Privacy Code.

Celo

Celo, accessed through a mobile app installed on a mobile device or via the desktop app, provides a real time secure messaging service:

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. A patient consent process for the capturing of images which is described further below

The Patient Information

The patient information will primarily be images of the patient anatomy and messages related to the patients care and treatment. The information will include the NHI and other identifiers including: first name, last name, DOB and Gender.

Privacy and Confidentiality

1. **Login**

   The app must be accessed through the clinician logging in with their unique login, I.e. Secure access. This enables the clinician 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 clinician cannot access other information stored for patients whose care they have not been involved in.

2. **Patient consent**

   The application contains a digital consent process which has been developed with input from clinical organisations including leading New Zealand District Health Boards. The digital consent process ensures that patient consent is obtained for taking and use of clinical images and is obtained before those images are taken, wherever possible. If patient consent cannot be obtained (e.g. because the patient lacks capacity or is unable to give consent e.g. the image needs to be taken during an operation) then consent is sought following the image being taken, when the patient is able to engage.

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 utilising Microsoft App services. Microsoft spend over $1 billion on cyber security per annum.

   Patient information can be retrieved by request of the patient to the clinician that is caring for them. Celo is not an electronic medical record, but is a secure healthcare collaboration tool that allows clinicians to move away from sending patient information by inappropriate methods such as WhatsApp, email or text message.

   In the event of any security breach relating to Microsoft Azure or Celo, Celo will notify the customer directly.

Appendix A
Security Overview

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 healtchcare network

Celo features an Authenticated Healthcare Directory. 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 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.

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.

Microsoft

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, 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.

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.

ISO AICPA SOC 2

Appendix B
Celo: The compliant alternative to WhatsApp in the Healthcare Setting

Introduction

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".

Appendix B
Celo: The compliant alternative to WhatsApp in the Healthcare Setting

Celo solves healthcare privacy risks

Authenticated
All Celo users are verified as healthcare professionals working at a verified healthcare organisation. The Celo app is always pin code or biometrics protected.

Secure
All Celo data is stored securely on Celo 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 clinicians 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

- The reason most messaging apps are free is because the users information is being sold to third parties.
- 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. All Celo users are verified healthcare professionals.

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 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 Directory.

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.