Smart Oncology Network (SONet)

Data Use & Privacy Statement

NZSO members interested in participating in the SONet Project will be interested in how the data generated from their use of the Celo App can be used. The Celo Guidelines of Use and Terms and Conditions[1] provides detailed information about who owns the data, how it can be used, the permissions required and how it is stored.

Roche NZ has no rights to access, view or use any information transmitted using the Celo App.

For the purposes of reviewing the success of the SONet Project, Celo will produce generic reports containing information such as, the number of messages sent, the number of users active within the NZSO organisation, the number and types of documents shared, and the volume of communication between users and within each research group. No user-identifiable information will be included in any report.

Reports will be shared with groups who participate in the SONet Project.

Celo Terms and Conditions: Clause 3.6

- *All information that is transmitted using Celo remains property of the user organisation (e.g. NZSO), this includes but is not limited to patient information.*
- *All patient information is protected using Celo's leading best practice security measures and access to customer data by Celo and/or its contractors is audited and only for providing the Celo services.*
- *Any access to customer data in the provision of Celo services is encrypted and therefore no actual content of customer data is available unless audited in accordance with customer permission and/or legal authority to do so.*
- *All Celo information is stored in an encrypted state including images.*
- *Celo information is only accessible to Celo users that have authorisation to view that information and is logged accordingly.*

Additional security information

1. **Device Security** – users must provide a pin to access Celo. Nothing is stored on the local storage of the device. Inactivate remotely.
2. **Transmission** – all transmission is encrypted during the journey with healthcare grade encryption preventing a "man in the middle" attack.
3. **Storage** – All Celo information is stored in a Microsoft Azure, Australian located and trusted server.
4. **Integration** – Celo allows integration with Electronic Medical Records. This improves patient safety and allows auditing. Integration via RESTful APIs
5. **Capture** – All photographs captured within Celo are done from within the App. This treats Celo as a fully standalone system. All photos are watermarked with patient and user information as well as a timestamp.
6. **Consent** – Celo allows a fully customisable consent system. Organisations can set their consent template and users can capture patient consents for clinical imaging via sign on glass.
7. **Authenticated Network** – All Celo contacts are authenticated which prevents any unauthorised users from being on the system.

For more information, go to the Celo web site (www.celohealth.com).

1. https://www.celohealth.com/wp-content/uploads/2017/01/Celo-Guidelines-of-Use-Terms-and-Conditions.pdf