



Data Security

We are very committed to protecting citizens and their privacy and follow a strict best practice security and privacy policy.

Is Corti's solution HIPAA or GDPR compliant?

Yes. We rigorously follow the most up-to-date best-practices and are able to live up to HIPAA compliance guidelines when needed. As of May 25th, 2018, the EU General Data Protection Regulation (GDPR) went into effect, and our GDPR specialists work tirelessly to ensure full compliance..

Is Corti's solution redundant?

Yes. We work in a critical environment in which failure is not an option. This is why we have built our entire solution, i.e. database infrastructure and interfaces, to be 100% redundant in case of sudden technical problems or emergencies.

How do you keep the data secure?

Security is ensured through data encryption, using FIPS-approved encryption standards, including AES256. Data is stored in an AES256-encrypted database, which is protected by multifactor authentication with full-access audit logging.

How do you control who works on the data?

Data scientists have their own authentication credentials to access data, and they are only granted access to datasets on a case-by-case basis if deemed necessary by our Chief Technology Officer. Furthermore, we deploy access control, regular security updates, and employee NDA's to keep the data secure.

How do we control disclosure and data management?

In addition to our strict security measures, we sign a mutual NDA with any new partner to ensure clear lines about what you and we can and cannot do with any data exchanged during our collaboration.

For more information, contact info@corti.ai.