www.iCarol.com
1-888-4-iCarol
info@icarol.com

Security and Privacy of Your Data

Members of your community trust you with their personal information. You can be assured that, along with your internal confidentiality and privacy policies, iCarol is working behind the scenes to provide you the best electronic security we can. There's nothing we take more seriously than being good stewards of your data.

Physically Secure Data Centers

iCarol uses advanced, highly secure facilities for reliable operations.

- Fire suppression
- Access limited to approved personnel only
- Entrances/exits electronically secured with CCTV monitoring

Disaster Recovery/Business Continuity

- Tier 3 data centers
- Primary data center with "hot" backups ready to take over in under a minute
- Ongoing data backups for file servers and databases
- On-site generators for power loss
- Backup fuel store for power generators
- Connections from multiple Telcos to ensure connectivity

Data Privacy and Security within iCarol

- 2048-bit SSL encryption for data "in transport" to/from iCarol, to/from users and help seekers, for both wired and wireless mediums*
- AES256-bit encryption for personally-identifiable data "at rest" (when stored in the database)
- Unique user IDs and passwords
- Single-sign-on available
- "Shred" or delete personally-identifiable data while retaining non-identifiable data for reporting
- Prevent access to view identifiable data through advanced security settings, certifying access by selected machines/locations, and by data partitioning

Process Safeguards

- Annual risk assessment for HIPAA and GDPR
- Ongoing confidentiality training for staff
- Annual vulnerability scans with resolution of high and medium findings
- Regular "failover tests" to backup data centers and test restoration of data backups
- Regular reviews throughout the year with legal compliance experts, Development, and IT personnel
- Data centers audited and certified for multiple areas, including SSAE-16; SOC 2, type 2; PCI DSS, and more

iCarol Security Summary

- End-to-end data encryption for both wired and wireless mediums*
- Encryption for data "at rest" in the database
- Tier 3 data centers with at least 99.982% availability
- Dynamic disaster recovery
- Regular vulnerability scans
- Regular risk assessments for HIPAA and other privacy-related regulations in Canada and the EU

*The single exception: Text messages are "in the clear" and readable when traversing the carrier network