iCarol: A Security Summary

Updated July 2016 | http://www.iCarol.com

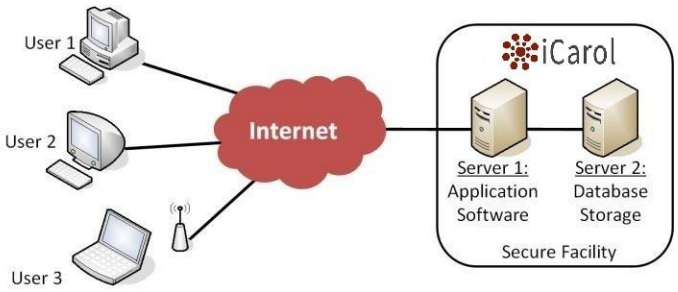
iCarol offers secure service to helplines using web technology. We understand that our clients need confidentiality applied to the people, processes, and tools used to run their operations. As a result of our security measures, you can rest assured that iCarol protects your information from access by unauthorized individuals.

Comprehensive security

The following measures apply to all aspects of iCarol's systems, including our secure web-based user interface and iCarol Messaging (including live chat and texting/SMS). Once data leaves our infrastructure to a user's computer, mobile device, or to be carried over mobile carrier's SMS network, it is the responsibility of those parties to provide and enforce their own security measures.

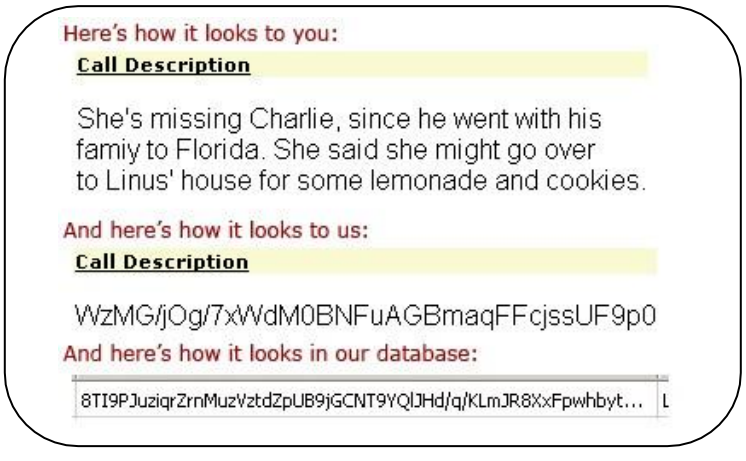
Audited Security Measures

iCarol is routinely audited to demonstrate compliance with the strict standards of the Payment Card Industry (PCI) association. In doing so, it reaches the same level of security that is required for transactions among the major international financial institutions. We achieved this by applying security best practices across our entire infrastructure – from the time it leaves your computer all the way to the hard drives on our servers.



Secure Communications and Data Center

While using iCarol, all data from any user's computer travels in a completely encrypted format - the same technology used by banks, credit cards and online retailers (256-bit SSL encryption). iCarol runs in a facility that is physically and electronically secured from outside threats by certified professionals, 24 hours a day, 7 days a week, 365 days a year. And iCarol software employs numerous security measures to prevent unwanted or malicious people from gaining unauthorized access to information. (These techniques are described in more detail below.)



Secure Storage

Sensitive data is stored in encrypted format on the hard drive

iCarol stores sensitive caller information in the database in an encrypted format, so that only authorized users from your agency will be able to access and read it. **Not even our staff sees the**

information about calls and callers in the database without being authorized by you. The specific fields that are encrypted in this manner are: Caller Name, Caller History, Instructions About The Caller, Call Narrative, Feedback On A Call, and Staff Feedback About A Call.

iCarol Technical Safeguards

- 256-bit SSL encryption from user's computer to the secure data center – regardless of transmission medium (wired or wireless)
- Unique usernames for each user, and password protected entry
- Passwords are stored in encrypted and hashed (unreadable) format
- All sign ons are logged with date, time, username and IP address so that access can be audited
- Administrators from the client agency can deactivate any user's account, preventing that person from signing on. User accounts can also be deleted, which removes all of their past activity from iCarol immediately
- After a few hours of inactivity, users must sign on again to access iCarol
- Phone workers on untrusted computers can be prevented from viewing call and caller information (i.e. from home or work)
- Call and caller-sensitive data is stored in the database in encrypted format only readable by the client's authorized users. This data can be automatically deleted from the database after a period designated by the client (typically 90 days), if so set by someone at your agency with administrative security

Advanced facility for secure and reliable operation

The "data center" that houses iCarol has extensive physical and electronic security, as well as state- of-the-art systems to ensure it stays up and running. This includes:

- Secure backups of application files, held on site as well as in a secure off site location
- Database backups performed at least every 15 minutes and held on site and off site
- Standby servers in geographically disparate locations ready to take over in the unlikely event that the primary systems fail (High Availability)
- Hosted in an SSAE16 certified data center
- Advanced power, cooling and security systems to ensure 24/7 operations.
- 24/7 uniformed security guards and a man-trap at the entrance to building
- Industry-leading network availability using a multi-carrier network of ISPs to provide network redundancy.
- On-site diesel generators are tested regularly and can run indefinitely if power feeds fail
- Two 4000/5000KVA transformers fed by dual underground 13.8 Kv feeder lines from fault-tolerant substations
- An advanced multi-zoned, pre-action, dry-pipe fire-suppression system protects the data center in the unlikely event of a fire
- Entrances and exits are electronically secured and monitored via closed-circuit cameras
- Data centers are only accessible to qualified network and data center technicians

Compliance with privacy laws

We at iCarol are acquainted with privacy laws like HIPAA (US), PIPEDA (Canada), and the Data Protection Act (UK and Europe). We have safeguards and processes so that we do our part to maintain compliance with these laws, and are willing to sign needed agreements asserting our role in your compliance with them.

Conclusion

We know that protecting confidential information is paramount to non-profit helplines. This is why we've invested heavily in top-of-the-line technology to keep your data as safe and secure as possible, from your computers to our servers. With iCarol's expertise, and highly trusted and tested approach to data protection, the cloud is the safest place for your organization to be.

Contact iCarol today to find out exactly how we can keep all your data safe and help you abide by privacy laws relevant to your industry.