UP IN THE AIR

about your data in the cloud?

At our agency, we use the ReporterBase system to manage our business, which includes your depo schedule, notices, transcripts, exhibits, other files you entrust to us, invoices, and statements. The latest version, ReporterBase 9 (RB9), is a cloud-based system, meaning the application and files are stored remotely, not in our offices. If you are wondering why we do this and how safe your confidential information is with us, we have compiled this overview of why we are in the cloud and the security measures taken with your data in the cloud.

Cloud benefits

With our database and client files in the cloud instead of our offices, we can provide better service. Some highlights:

- Storing information virtually eliminates the need for paper copies and file cabinets. Accessing information is quicker and easier. And no worries about lost or damaged files.
- We can access your data and repository files from anywhere we have an Internet connection. If we have to evacuate our offices for any reason, we can continue to provide service because everything is online.
- The cloud platform we use makes duplicates of your data in real time. This is better than any backup system: If the active server should go down, another server takes over with no loss of data — and no downtime.

The cloud platform where your information is stored

RB9, the information we enter into the system, and your files we upload to the system are all stored on Microsoft Azure Cloud Services, one of the best cloud platforms for reliability, safety, and security.

1. Azure has a guaranteed 99.95% uptime, so we are basically never without access to information in the system.
2. Azure's high availability and redundancy processes duplicate our RB9 database on multiple servers in real time. Repository files are stored similarly with duplicates of files stored in several different physical places.
3. Safeguards in Azure are beyond what a single court reporting agency could provide. For example, Azure is HIPAA, TRUSTe, PCI DSS, and NERC CIP compliant. And because the file repository is also part of RB9, all of your case files entrusted to us are just as safe as your data entered in the RB system.
4. Microsoft has dedicated resources and processes that guarantee the security and privacy of data on Azure, earning a host of security certifications and following international standards for privacy controls in the cloud.

Microsoft is a leader in cloud security and data privacy. They were the first cloud provider recognized by the European Union's data protection authorities for their commitment to EU privacy laws, and the first major cloud provider to adopt the international cloud privacy standard, ISO/IEC 27018. Azure maintains the largest compliance portfolio in the industry, complying with numerous other national and international data privacy acts. We can provide details upon request.

RB9's security protocols

Security is always important when dealing with sensitive and critical information, such as the information you entrust to us. So RB9 follows general security rules for business applications and online services. For example, users are automatically logged off after a set period of inactivity.

Data and files stored in RB9 are safeguarded by methods chosen for their appropriateness and security standards. For example:

- RB9 allows access only via TLS 1.2. Other security protocols, such as SSL and TLS 1.1/1.0, are outdated and vulnerable, so they cannot access RB9.
- RB9 stores user passwords using a secure hash algorithm so no one can decrypt passwords.
- RB9 stores sensitive data, such as birthdays, SSN, and Tax ID, using a 256-bit algorithm. If someone steals the data, they cannot decrypt the data even if they know the password.
- The SQL Servers in the cloud where your data resides cannot be accessed from the outside. And the RB9 Application Server is designed to be accessed using the RB9 application only, so access to customer data is not possible without the application. Similarly, client repository files cannot be accessed from outside. They can only be accessed through the RB9 application.
- RB9 is more secure than an in-house system in other ways. For example, RB9 doesn't require open ports to transfer data like other applications. The database where your information is stored is not exposed to the internet nor do we keep any custom ports open for file downloads.
- In RB9, we control every staff member's access to data and file repositories with multiple permission levels. Each user has access only to areas they need to complete their work. That is further restricted to view only or edit options depending on a person's job responsibilities.

Login security is key

A key area of security for any application that handles sensitive information is the login process. RB9 contains a full range of security protocols for login including:

- Complex passwords
- Automatic account lockout after a certain number of incorrect password tries
- Required periodic password resets
- Two-factor authentication (2FA is a more secure way to confirm a user's identity by adding a second factor to signing in, such as a code sent to their cell phone that they must enter after their user name and password.)
- Password controlled by users only (Passwords are not accessible by system administrators or OMTI personnel. And users can reset their passwords at any time.)

OMTI is our trusted supplier

OMTI has been providing court reporting agencies with business management software for over 35 years. They are the largest provider in this highly specialized market with hundreds of clients in the US and Canada. They have earned our trust and the trust of the industry by being a reputable service provider.

Our RB9 data is not stored at OMTI. OMTI does not host files on their own servers. They developed the RB system, maintain it, and provide us with support in using it. We enter data and upload files through RB9 to Microsoft Azure's servers in the cloud, not OMTI's servers, so your information remains confidential. We maintain control of your data and files.

OMTI provides a couple of additional layers of data protection beyond what the Azure platform provides:

1. OMTI maintains a several-day backup of all RB data. This data is encrypted and stored separately, and would be used in the case of the 0.001% chance that all our servers on the Azure platform crashed at the same time.
2. OMTI maintains user access logs that record the date, time, URL executed on, operation performed (created, updated, deleted) and client IP address. Passwords are not logged under any circumstances. If there is suspicion of inappropriate access, OMTI can provide us with these log entry records to assist in forensic analysis. Logs are kept for a minimum of 90 days in a secure area to prevent tampering.

In addition to the specific examples earlier, OMTI has developed a complete set of policies and procedures for maintaining the safeguarding aspects within their specific workflow. In an ongoing process, they analyze their risk environment, evaluate their controls, and identify and remediate any gaps discovered during this process. They also have documentation to cover all of their policies and procedures.

OMTI is SOC 2 Type 2 compliant

To reassure users of OMTI services that their information is secure, OMTI underwent a SOC 2 audit. SOC 2, the voluntary compliance standard for service organization developed by the American Institute of CPAs (AICPA), specifies how organizations should manage customer data, especially when that data is managed in the cloud. SOC is short for System and Organization Controls. It provides an independent assessment of a company's security and privacy controls environment.

There are 2 versions of SOC 2 compliance reports. Type 1 is basically a snapshot in time that shows a company has policies in place to address SOC 2 areas. The Type 2 report details the results from the auditor observing a company for a period of time to check that they not only have proper security policies and protocols but follow them. This is the type of SOC 2 audit that OMTI underwent.

Their first SOC 2 audit was completed June 30, 2022 by Johanson Group, LLP. They found OMTI to be compliant with no exceptions, which is the best finding in these independent third-party audits. Their SOC 2 certification shows that all relevant systems at OMTI or otherwise under OMTI's responsibility are properly protected against the threat of modification or unauthorized access.

Security and compliance are ongoing efforts, so OMTI continues to monitor their policies, procedures, and internal compliance. And they will continue to submit to SOC 2 audits annually to provide proof of their compliance.

Using our online offices is safe & convenient

If you wonder about the safety of accessing your depo calendar, case files, and invoices online, you can be assured when using our online offices that they have the same security features as we have for RB9. So you can enjoy the convenience of 24/7 access without worry.

Our online offices also offer you the same benefits we have in regards to storing and using data in the cloud, such as reducing your use of paper copies and accessing your information anywhere you have an internet connection. Plus:

- Online case repositories. View and download job and case files, including streaming video.
- Depo calendars. Look up upcoming, canceled, or previous depos (and other types of jobs), and view any job's details, including directions to the location via Google, Mapquest, or Bing maps.
- Request services with as much detail as you want or as little as a depo's scheduled date and time. Upload related files like notices.
- Cancel or reschedule jobs.
- Backorder transcripts.
- Download transcripts, files, invoices. Our RB-PDF Transcripts are readable in Adobe Acrobat so you don't have to purchase and maintain a separate transcript application.
- Work with transcripts and their related files online with our interactive Transcript Packages. You can highlight and make notes on the transcripts and export transcripts and notes in a variety of formats, including AMICUS, condensed, and archival PDFs.
- Pay invoices online. Look up outstanding amounts and other invoice details including previous payments.

You can also access our offices on your smartphone safely

Maybe the most convenient way to make requests and find information is with your smartphone. But you don't have to call us: Accessing RB Connect on your mobile device provides the same protections as accessing it on a laptop or other computer because in both instances you access RB Connect through the browser on your device.

RB Connect on your phone looks different because it has a user interface designed for the smaller screens of mobile devices, but it includes all the same safety features. So you don't have to boot up your computer or play telephone tag with us; you can find what you need quickly anytime. The only things you can't do on your phone are upload files or pay invoices.

Still have questions?

If you would like more information about the security of our cloud-based management of your confidential information, please contact us. We can provide you with documentation about Azure's security and privacy measures, OMTI's security protocols and system architecture, and RB9 security features plus answer any questions you have about our in-house processes to protect your confidential information.