Last Updated: June 2022

Your privacy and security are paramount. This privacy statement explains how we protect the data you enter into our SaaS product, CAC CareNet. OMS Technologies, Inc. only collects personal data from its users that is needed to aid in training, support, and updates, this includes the users name, email address, and phone number. We do not collect personal data for marketing purposes.

Through the Minimum Necessary Standard, the data is protected. By way of SOC2 Compliant, Government Privacy rated servers and our partnership with AWS, our data is protected from an outside entity, data mining or a breach through end-to-end Encryption.

Each Client and member of our staff are required through series of 'doors' including passwords and two factor authentication to authenticate both their person and the device that they are using. This is followed up with a log of all persons who access, change, or utilize a specific database and in most cases specific pieces of information within a protected clients file.

Contact us if you have a privacy concern, complaint, or any questions for the OMS Technologies, Inc. Chief Privacy Officer. You can reach us at privacy@omstinc.com, or support@omstinc.com for general support. You can also contact OMS Technology for more information, or any other concerns, by phone at (405) 701-0295. M-F 8 am – 5pm (CST).

We do not collect Personal data

OMS Technologies, Inc. only collects contact information as stated above. We do not collect personal data from any of our users. Our concerns are solely focused on protecting your data, and your privacy, and not marketing efforts.

Cookies and Tracking

We do not utilize Cookies in CAC CareNet. We do not track users for any marketing purposes.

Services provided by your organization—notice to end users

If you use an OMST product, specifically CAC CareNet with an account provided by an organization you are affiliated with, that organization may:

- Control and administer your CAC CareNet account, including granular permission setting, roles, abilities, and access to portions of the software.
- Access and process your data, including data collection, for case management, reporting, and long-term storage.
- User passwords are one-way encrypted in our database and can't be accessed or used by anyone even if the encrypted password was compromised. Because of this encryption if you loose access to your account password the only way to recover this is through an account administrator, or by contacting us directly at support@omstinc.com.
- If your access is halted, to your work account (in event of change of employment, for example), you will lose access to all work you were involved in while in their employ. If access is needed, you must directly request reinstated access to CAC CareNet from your organization's Director. It is at their sole discretion whether to grant you access again.

OMS Technologies, Inc. account, i.e., CAC CareNet

CAC CareNet is designed to protect the data at all costs. Only those who have been giving active credentials, by their Administrator or Director will have access to the data. Further, most users will have limited access, based on their needs to fulfill their position with the organization. The highly granular security access levels allow for data protection from all working in the CACCN service. i.e., a person may be granted access to all records, and yet can be excluded from seeing certain records with our Record Locking.

The only way OMST staff will access the data is by the client requesting that we log in using their credentials. In such cases, written permission is mandatory. will only allow necessary personal to have any access to our clients' personal information. In addition, our development team has provided 'locks', locked records, segmentation and Tiered Security Grouping that allows for both our OMS Team in addition to our clients to specifically control and minimize the amount of data that everyone can view, change and delete.

Collection of data within CAC CareNet

All data stored and used on using the CAC CareNet software is solely owned by client agency and cannot and will not be accessed by any other persons or agencies. The data captured and saved within CAC CareNet can ONLY be viewed/accessed by

those with credentials granted from the Organization. The only way an OMS Technologies, Inc. employee (OMST employee) can access is by request of the user, using their credentials. OMST employees do not have access to the data stored. If an attempt were to be made by an OMST employee, to utilize credentials shared with them, it will log the access in the Client/Organization's History and Audit trail. Administrators can view the Audit History at any time, and/or request reports from OMST at no cost to them.

Reporting and review of any breaches, inconsistencies

Every instance of misuse or a breach of data or even the notice of any inconsistencies are immediately reviewed and evaluated by our privacy and compliance team.

Mitigation of any harmful disclosures that have occurred during the use of the database and reporting this information to our clients based upon policies and procedures and the Privacy Rule. Additional reporting would occur with any significant breach or incidental use in accordance with Federal Privacy Laws.

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we store your data, and how long we retain your data. You can find more information on OMST and our commitment to protecting your privacy and data. At OMS Technologies, Inc., we value, protect, and defend privacy. We believe in transparency, so our users and organizations can control their data and have informed choices, including best practices, in how it is used.

CAC CareNet-specific details:

Our CAC CareNet software as a service (SaaS), designed by CACs across the country, is continuously updated and improvements made to our service as a part of your subscription fee. The updates often include new features to the service as well added security to your service. For CACCN to give you the best possible experience, and safeguard your data, we include the following with your Subscription:

- Personalized training on how to use the service, including best practices, and HIPAA guidelines.
- Ongoing support and service as needed
- New features to CACCN, with training materials, or live training, and client preferences.
- Regular and repeated backups, multiple times a day, week, and month. The backups are saved for a minimum of 4 months.

In the event of a conflict between this OMS Technologies, Inc. privacy statement and the terms of any agreement(s) between a Client and OMS Technologies, Inc., the terms of those agreement(s) will control.

General Information re. Privacy and Security Measures

When a Client subscribes to CACCN, they have a safe and secure place to enter data, run reports, share with other agencies, and/or law enforcement. The subscription includes global improvements, security upgrades, and adding new features. Regarding data collection that OMST does save -

- When a Client engages with an OMST Sales Specialist, we collect the Client's name and contact data, along with information about the Client's organization, to support that engagement.
- When a Client interacts with an OMST Support Professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When OMST sends communications to a Client, we use this data to personalize the content of the communication.
- When a Client engages with OMST for professional services, we collect the name and contact data of the Client's designated point of contact and use information provided by the Client to perform the services that the Client has requested.

How the data is handled

- When data is uploaded it is SSL- encrypted up- then stored in S3 buckets on AWS HIPAA and SOC 2 certified servers.
- When data is downloaded it is SSL encrypted and stored directly on the client's hard drive.
- The active data is stored and served on AWS RDS database servers that are behind a bastion server and are HIPAA and SOC 2 certified storage servers.
- Ability to access the data- data access is granted by the Administrator or Director of the organization. This can be changed or revoked by the Administrator only.
- Access can be so granular that even the person uploading a document, may not have permission to view it again later.
- Our training for clients includes best practices for safeguarding the data on their end.

- We secure your data at rest and in transit.
- Training regarding procedures and on best practices is given to the Clients during their initial training.
- Our staff is given annual training on the processes and procedures for HIPAA and how to follow the SOC 2 standards.