

Privacy Policy Statement

Unique Software Solutions, Inc. (USSI) is committed to your privacy. By taking extreme care in protecting any information we receive, we ensure that information is protected when we host your data on our servers as well as when we provide technical support or receive information on our website.

Our USSI Website, <http://www.ohmsoftware.com> and our OHM/ASP™ service, which utilizes the Occupational Health Manager® (OHM) database, are housed on secure web servers owned solely by USSI and located in our facility in Colorado Springs, Colorado. Providing a secure, protected and environmentally controlled data center is of utmost importance to us as is providing state-of-the-art equipment for optimum functionality.

For those of our customers who choose to host their Occupational Health Manager® database through USSI, whenever the term "Customer Information" is used in this Statement, it refers to the information about your employee/patient records stored on our protected servers.

USSI warrants that the Customer Information housed on our protected servers will not be accessed without written consent of the previously approved company contact. As such, this information will not be available for the purposes of marketing to, or otherwise communicating directly with, anyone listed in your database. Nor will USSI provide any information to a third party, unless we are required by law to do so.

Cookies

A cookie is defined as a small text file containing a unique identification number that is transferred from a web server to the end user's browser, enabling the serving party to track the website activities of the end user. USSI's OHM/ASP™ service utilizing the OHM/Web™ software database does not issue any cookies that enable third parties to track the activities of our end users; however, our software does contain cookies that allow you to track end users activities. An option is available within the system allowing the end user to turn cookies off as desired.

Security

USSI's OHM/ASP™ Data Center consists of DELL state-of-the-art equipment that provides uninterruptible power supplies (UPS), load balancing, 100 Mbps network connectivity, back-up generating capacity, off-site disaster mechanisms and secure back-up storage along with multiple levels of security. A series of automated e-mails and immediate alerts are submitted to the on-duty technical staff in case of any abnormalities in our web server environment. Redundant, multi-level networking ensures security from any type of power outages or natural disasters.

No single point of failure is possible. Availability is ensured through backup procedures allowing access even if component failures occur or the unlikely event that the entire Internet was to go down.

Physical access to the OHM/ASP™ servers is limited to four key USSI personnel (Director of Technical Support, Director of Sales, President and CEO). One of these key individuals must be present before ANY access is granted to other staff e.g. technical support staff. Of these four key personnel only the President and CEO have administrative rights to the servers housing client data. Strict internal controls over staff members with access to Customer Information are maintained by USSI. Such access is granted only on a need to know basis. USSI performs criminal background checks on all technical personnel.

The OHM/ASP™ data is housed on servers kept in a server room accessible only by authorized USSI personnel. To further protect the data while being transferred off site, backup tapes are created in an encrypted format; only the system administrator has restore rights to the tapes. The data is transmitted using 128-bit SSL encryption technology to ensure confidentiality of the data on the network.

Correction/Updating of Customer Information

When utilized as an ASP service, our software is developed to work as a database for tracking company employee health, safety and environmental data and/or patient and associated billing data. This information is updated solely by the end user and is not viewed, written to, printed or deleted by USSI without the express written consent of the authorized end user. The end users control access to their data eliminating the need for access by USSI employees unless an authorized administrator who has been identified by the end user, requests specific technical assistance and provides a temporary login to a USSI Technician.

European Data Protection Directive

USSI currently commits and will continue to make every effort to comply with the principles of the EU Data Protection Directive 95/46 and any successor legislation, in relation to any "personal data" received from the end user, to the extent that the Directives apply to "database service providers".

USSI also contractually commits to compliance of all reasonable technical and organizational measures required to keep such personal data secure and to protect it against accidental loss or unlawful destruction, alteration, disclosure or access; and to deal with the information only in accordance with reasonable and lawful instructions.

Changes to Privacy Policy

This policy may be updated from time to time by USSI; updating is reflected by the revision date at the bottom of this statement.

Contacting Us

Should you have any questions or concerns regarding this policy, please contact us at SpecialService@OHMSoftware.com.