Whos On. Location
An MRI Software Company

Security

Contents

WhosOnLocation Security

Customer data is one of the most valuable assets your company has which is why our top priority is delivering a high-performance solution with a focus on keeping our customers' data safe and their interactions secure.

WhosOnLocation understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Data Protection & Security

WhosOnLocation is hosted in AWS data centers that have been certified as ISO-27001, PCI/DSS Service Provider Level1 and/or SOC II compliance. Our global Security Team is on call 24/7 to respond to security alerts and events. We are committed to protecting the security of our customer's information.

Availability & Continuity

We maintain a publicly available system status web page and employ service clusters and network redundancies to eliminate single points of failure. Backed by a Disaster Recovery program that ensures our service remains available or are easily recoverable in the case of a disaster.

Product Security Features

We make it seamless for customers to manage access and sharing policies with authentication and single sign-on (SSO) options. All communication with our servers is encrypted using industry standard HTTPS over public networks, meaning the traffic between your account to WhosOnLocation is secure.

ISO, Compliance & Certifications

We utilize best practices to achieve and maintain compliance with industry accepted general security and privacy frameworks, which in turn helps our customers meet their own compliance standards.

Employee Security

We operate a comprehensive set of security policies that are shared with all employees and contractors. Background checks are performed on all new employees. All employees and contractors sign non-disclosure and confidentiality agreements.

Data Protection & Security

WhosOnLocation is committed to helping protect the security of customer's information. We have implemented, maintained and followed appropriate technical and organizational measures to protect our customer's data against accidental, unauthorized or unlawful access. Ensuring your customer data is not disclosed, altered, lost, or deleted.

Domain	Practice
Organization of information security	Security Ownership. WhosOnLocation has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. Security Roles and Responsibilities. WhosOnLocation personnel with access to Customer Data are subject to confidentiality obligations.
Risk analysis	WhosOnLocation continually performs risk analysis to achieve the highest level of security. Security concepts and techniques have been integral to our solution's design right from the beginning and we continue to invest heavily in security improvements for our product, process, people, and technology. We perform full security audits of our product and infrastructure regularly, including third-party audits at least annually. Our risk assessment process aligns with the OWASP standard.

Physical Security

Domain	Practice
Cloud hosting facilities	WhosOnLocation hosts service data in AWS data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance. Learn more about AWS ISO Compliance here. AWS infrastructure services include back-up power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data.
Location	WhosOnLocation leverages AWS data centers in the United States, Europe, and Asia/Pacific.
On-site security	AWS on-site security includes a number of features such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. AWS data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC 2 compliance. Learn more about AWS physical security.
Monitoring	All Production Network systems, networked devices, and circuits are constantly monitored and logically administered by WhosOnLocation staff. Physical security, power, and internet connectivity are monitored by AWS.

WhosOnLocation offices	WhosOnLocation utilizes physical access controls within its own facilities including limiting employee access via our access control system, awareness alerts of entry after hours (even by authorized personnel), and entrance monitoring on camera. We also limit visitor and contractor access through our visitor management system. Limit integrated door opening to office hours and then only if the host is present and there are at least ‘x’ employees on-site.

Application Security

Domain	Practice
Dedicated Security Team	Our global Security Team is on call 24/7 to respond to security alerts and events.
Protection	Our network is protected through the use of key AWS security services, regular audits, and network intelligence technologies which monitor and/or block malicious traffic and network attacks.
Architecture	Our network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in our most trusted zones. Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply.
Network vulnerability scanning	Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.
Vulnerability testing	WhosOnLocation.com tests all code for security vulnerabilities before release and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly: • Application vulnerability threat assessments

	• Network vulnerability threat assessments • Selected penetration testing and code review • Security control framework review and testing
3rd-Party vulnerability testing	If you would like to run your own 3rd-Party Vulnerability Test against WhosOnLocation please send an email to trust@whosonlocation.com (Please note customer-driven and requested vulnerability tests are at the customer's cost.
Threat intelligence program	WhosOnLocation participates in several threat intelligence sharing programs. We monitor threats posted to these threat intelligence networks and take action based on our risk and exposure.
Logic access	Access to the WhosOnLocation Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the WhosOnLocation Production Network are required to use multiple-factors of authentication.
Security incident response	WhosOnLocation maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification by WhosOnLocation is described Clause 18 Security Incident Notification of our Master Subscription Agreement.

	In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.
Access control	All access to data within WhosOnLocation is governed by access rights. Every user who attempts to access your WhosOnLocation account is authenticated by username and password. The administrator of your WhosOnLocation instance may define granular access privileges to individual users, and email notifications alert administrators when someone is granted admin access. Our security architecture ensures that each request to WhosOnLocation is accompanied by user identity credentials to ensure segregation of customer data.
Application security	WhosOnLocation maintains a robust application audit log, to include security events such as user logins or configuration changes. Additionally, WhosOnLocation follows secure credential storage best practices by storing passwords using the bcrypt (salted) hash function.

Information Security

Domain	Practice
Encryption in transit	Communications between you and WhosOnLocation are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS) over public networks. TLS is also supported for encryption of emails. This ensures that all traffic between you and WhosOnLocation is secure during transit. Unlike email-based communication, most of which flows unprotected over the Internet, your communication with WhosOnLocation is completely protected.
Encryption at rest	Customers of WhosOnLocation benefit from the protections of encryption at rest for their data.
Asset management	**Asset Inventory** WhosOnLocation maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to WhosOnLocation personnel authorized in writing to have such access. **Asset Handling** WhosOnLocation imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. WhosOnLocation personnel are prohibited from storing Customer Data on portable devices, remotely accessing Customer Data, or processing

	Customer Data outside WhosOnLocation's facilities unless authorization is received from the Customer to do so. WhosOnLocation imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. WhosOnLocation personnel are prohibited from storing Customer Data on portable devices, remotely accessing Customer Data, using Customer Data for testing/training or processing Customer Data outside WhosOnLocation's facilities unless authorization is received from the Customer to do so.
Access Control	**Access Policy** WhosOnLocation maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** • WhosOnLocation maintains and updates a record of personnel authorized to access WhosOnLocation systems that contain Customer Data. • WhosOnLocation deactivates authentication credentials that have not been used for a period of time not to exceed six months. • WhosOnLocation identifies those personnel who may grant, alter or cancel authorized access to data and resources. • WhosOnLocation ensures that where more than one individual has access to systems

	containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** • Technical support personnel are only permitted to have access to Customer Data when needed. • WhosOnLocation restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** • WhosOnLocation instructs WhosOnLocation personnel to disable administrative sessions when leaving premises WhosOnLocation controls or when computers are otherwise left unattended. • WhosOnLocation stores passwords in a way that makes them unintelligible while they are in force. **Authentication** • WhosOnLocation uses industry standard practices to identify and authenticate users who attempt to access information systems. • Where authentication mechanisms are based on passwords, WhosOnLocation requires that the passwords are renewed regularly. • Where authentication mechanisms are based on passwords, WhosOnLocation requires the password to be complex. • WhosOnLocation monitors repeated attempts to gain access to the information system using an invalid password.

	• WhosOnLocation uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design** WhosOnLocation has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Human resources	**Security Awareness:** WhosOnLocation has developed a comprehensive set of security policies covering a range of topics. These policies are shared with and made available to all employees and contractors with access to WhosOnLocation information assets. WhosOnLocation informs its personnel about relevant security procedures and their respective roles. In line with industry best practice for protecting the confidentiality of our Customers Data, all WhosOnLocation employees and agents agree to our Privacy Policy. Specifically, they agree and understand that Customer Data is the IP of the Customer and shall not be accessed without the prior written consent of the Customer, and/or copied, shared or disseminated to any Party without the prior written consent of the Customer. **Security Training**. All employees attend a Security Awareness Training which is given upon

	hire and annually thereafter. This includes informing personnel about relevant security procedures and their respective roles. The Security team provides additional security awareness updates via email, blog posts, and in presentations during internal events. WhosOnLocation also informs its personnel of possible consequences of breaching the security rules and procedures. WhosOnLocation will only use anonymous data in training. **Employee Vetting**: WhosOnLocation performs background checks on all new employees in accordance with local laws. These checks are also required to be completed for contractors. We also require all employees and contractors to comply with our Clean Slate policy where they must disclose any criminal record that occurs after engagement. We re-vet all employees and contractors annually. Cleaning crews are included. **Confidentiality Agreements**: All new hires are required to sign Non-Disclosure and Confidentiality agreements.

Availability & Continuity

Domain	Practice
Uprise	WhosOnLocation maintains a publicly available system-status webpage that includes system availability details, scheduled maintenance, service incident history, and relevant security events.
Redundancy	WhosOnLocation employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime and/or our Enhanced Disaster Recovery service offering allows us to deliver a high level of service availability, as Service Data is replicated across availability zones.
Business continuity management	• WhosOnLocation maintains emergency and contingency plans for the facilities in which WhosOnLocation information systems that process Customer Data are located. • WhosOnLocation's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-

	replicated state from before the time it was lost or destroyed.
Disaster recovery	Our Disaster Recovery (DR) program ensures that our services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, creating Disaster Recovery plans, and testing activities.
Data recovery procedures	On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), WhosOnLocation maintains multiple copies of Customer Data from which Customer Data can be recovered. • WhosOnLocation stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. • WhosOnLocation has specific procedures in place governing access to copies of Customer Data. • WhosOnLocation reviews data recovery procedures at least every six months.

	• WhosOnLocation logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. • Event Logging. WhosOnLocation logs access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Backups	Along with the regular file system snapshots, a full daily backup is taken of all systems and stored as a full point-in-time record.

Product Security Features

Domain	Practice
User authentication	Customers can enable native WhosOnLocation authentication, or Single sign-on (SSO).
Native authentication passwords	WhosOnLocation recommends strong password use. We offer three levels of Password Simple: minimum of 6 characters; Standard: (the default) minimum of 6 characters; combination of uppercase and lower case letters; Complex: (recommended) minimum of 8 characters, combination of uppercase and lower case letters; mixed with at least one number and one symbol (!, @, #, $, for example).
Password reset	Best Practice and security auditors recommend that to meet the minimum for compliance, with standards like OWASP, HIPAA, and Sarbanes-Oxley passwords should be changed every 45 to 90 days and should be different every time. The default setting is 'Do not force change'.
Multiple concurrent logins management	Enabling this option allows a single user to log in from more than one location at the same time. Disabling this option will automatically log out any prior sessions when a user logs in.

Role-based access controls	Access to data within WhosOnLocation is governed by role-based access control (RBAC) and can be configured to define granular access privileges. WhosOnLocation has various permission levels for users (owner, admin, reception, employee, service providers, end-user, etc.).
GDPR compliance	WhosOnLocation offers several settings to help your organization meet its GDPR (General Data Protection Regulation) compliance. **Under GDPR you must have:** • A disclaimer for visitor information capture. • A disclaimer for photo capture specifically. • The ability for a visitor to disable the system from remembering their details on sign in. • A way for visitors to see all information you have about them. • The ability to erase a visitor's information on their request. We have given you the tools to meet these standards through a combination of existing and new features. You can learn more about how we comply with GDPR here.

ISO Certification

Domain	Practice
Certification	ISO27001:2013 Information Security Management System.
Information Security Objectives	The following information security objectives have been defined for WhosOnLocation: • achieve and maintain compliance with ISO/IEC 27001:2013; • ensure WhosOnLocation meets its contractual obligations and complies with all legal & regulatory requirements, for example the General Data Protection Regulations (GDPR) • demonstrate top management support and continual improvement for information security; • maintain staff awareness of information security; • respond to information security incidents efficiently; ensure effective implementation of information security controls.
Scope	Information security management for design, development, deployment and maintenance of WhosOnLocation application services and infrastructure including operational support in line with Statement of Applicability.
Continual Improvement	The WhosOnLocation leadership team is committed to continual improvement of the information security management system. It is through the continual

	improvement process that the effectiveness of the ISMS processes will be assessed and improved. WhosOnLocation shall have a consistent approach to tackle identified nonconformities and take corrective action(s) to eliminate them.

Access to our ISO Documentation

Our ISO27001:2013 Certificate

Our certificate is available for download

Our ISO27001:2013 Policy Documents

As part of your evaluation of WhosOnLocation and to assist you with your audit of our standard operating procedures and controls, you can request copies of the following shareable policies by selecting the Request Documents button below and completing our request form:

- Information Security Policy
- Statement of Applicability
- Business Continuity Plan

Upon completing the form you will be directed to our NDA which must be agreed to. Upon receipt of your agreement to our NDA we will evaluate your request and if approved, confirmation will appear in your email inbox. Please allow up to 5 business days for your request to be processed.
Please note: WhosOnLocation reserves the right to 'not share' with you our ISO policy documentation should we determine that it is not appropriate to do so. We will inform you of that decision if applicable.

Request Documents

General Data Protection Regulation GDPR

WhosOnLocation has a rigorous process to ensure our software provides features that enable our customers (Data Controllers) to be GDPR compliant. These features include:

- The right of access
- The right to erasure
- The right to object
- The right to rectification
- The right to restrict processing
- The right to data portability
- The right not to be subject to automated decision-making including profiling.

How does WhosOnLocation support your GDPR compliance efforts?

- Your visitors data is kept private and is not shared with third parties.
- Your visitors have an option to be chosen ‘not to be remembered’.
- We give our customers tools for automatically deleting (or anonymizing) visitor data after a certain length of time.
- Visitor records can be rectified by your administrators on request by a visitor.
- Our customers can remove one, some, or all visitor records should they request that their details be removed from WhosOnLocation.
- You can create custom forms like ‘a consent and permission form’, an NDA, a Waiver, and/or a Privacy Policy (optionally with signature required) to ensure your visitor is aware of your policies, procedures, and use of their personal information.

International Traffic in Arms Regulation ITAR

International Traffic in Arms Regulations (ITAR) control the export and import of defense-related articles and services on the United States Munitions List (USML). According to the U.S. Government, all manufacturers, exporters, and brokers of defense articles, defense services, or related technical data must be ITAR compliant. Therefore, more companies are requiring their supply chain members to be ITAR compliant as well.
WhosOnLocation complies with ITAR through the following:

- Maintaining an information security policy
- Building and maintaining a secure network by installing and maintaining firewall configuration to protect data and avoiding the use of vendor supplied passwords and other security details
- Assigning a unique ID to each person with computer access
- Regular test security systems and processes
- Protect sensitive data with encryption
- Regular monitor and test networks
- Implement strong access control measures
- Track and monitor all access to network resources and sensitive data
- Maintain a vulnerability management program
- Implement measures to prevent the loss of ITAR controlled data

Customs-Trade Partnership Against Terrorism C-TPAT

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary supply-chain security program led by U.S. Customs and Border Protection (CBP) focused on improving the security of private companies' supply chains with respect to terrorism.

WhosOnLocation support the C-TPAT criteria through:

- Physical access control management for guest, contractors, employees and deliveries
- Information Technology Security | Password Protection

For detailed information on WhosOnLocations compliance with C-TPAT click here.

Good Manufacturing Practice GMP

Good Manufacturing Practices (GMP) is a system for ensuring that products are manufactured, packaged, and controlled according to industry quality standard. To put it simply GMP helps ensure a quality product.

WhosOnLocations helps organizations manage their compliance to meet GMP obligation including attendance tracking, hazard notice compliance, and induction management. For more info on GMP and WhosOnLocation click here.

FDA Food Safety Modernization Act FSMA

The Food Safety Modernization Act (FSMA) was enacted in 2011 to ensure food safety in the United States. FSMA aims to shift the focus toward preventing intentional adulteration of the food supply rather than responding to contamination. As such, requirements cover the mitigation of threats that make food production facilities vulnerable.
WhosOnLocaiton ensures that unauthorized visitors gain access to your facility. Ensuring everyone who enters the facility is authorized and accounted for.

- Verify visitor identity (photo capture, ID check, pre-registration) and deny access to those who are not permitted
- Maintain detailed real time reporting of entry, exist and sites accessed while onsite
- Require a valid purpose of visit and escort (host) upon sign-in
- Visitors sign any documentation needed to ensure they agree to onsite regulations and or NDA’s
- Contractors undertake inductions to comply with the site requirements and hold relevant and up to date insurances
- All visitor and contractor display badges
- Use zones within your organization to restrict access and accurately track access

TRUSTe Enterprise Privacy Certification

WhosOnlocation has demonstrated that our privacy programs, policies, and practises meet the requirements of EU-U.S Privacy Shield and/or Swiss-U.S. Privacy Shield. These companies have self-certified their participation in Privacy Shield with the U.S Department of Commerce at https://www.privacyshield.gov/list. TRUSTe verifies Privacy Shield compliance consistent with the requirements of the Privacy Shield Supplemental Principle on Verification.

California Consumer Privacy Act CCPA

About WhosOnLocation and the California Consumer Privacy Act

"The CCPA came into force on 1 January 2020 (called the “compliance date”), the Californian Attorney General won’t start enforcing it until 1 July 2020 (“enforcement date”). One of the key elements of the CCPA, amongst others, is that it focuses on transparency obligations and on provisions that limit the selling of personal information, requiring a “Do Not Sell My Personal Information” link to be included by businesses on their homepage.

Does CCPA apply to WhosOnLocation?

WhosOnLocation does not “sell” customer’s personal information, meaning that we also do not rent, disclose, release, transfer, make available or otherwise communicate that personal information to a third party for monetary or other valuable consideration.

WhosOnLocation also adheres to the highest standards for the capture, processing, and management of personally identifiable information and this includes NEVER sharing ANY information we capture from our customers or their 'data subjects'; employees, contractors and/or visitors. To read our full privacy policy, click here.

Because WhosOnLocation does not fall within any of the thresholds specified under the CCPA that determines whether or not we would be required to comply, the CCPA does not apply to WhosOnLocation today, however; we wanted to assure you that WhosOnLocation does take data privacy extremely seriously.

Our privacy commitment

We have designed our systems and adopted standard operating procedures to ensure we are compliant with the General Data Protection Regulations (GDPR). GDPR came into effect on 25 May 2018 and is one of the most comprehensive data protection laws in the world to date. We also undertake external auditing against our information security management systems and are ISO27001: 2013 certified. To review our full security statement, click here.

Ongoing monitoring

We will continue to review and monitor our adherence to CCPA and should our circumstances change we will take the necessary steps to adhere.

WhosOnLocation Employee Security

Security awareness

Policies - WhosOnLocation has a comprehensive set of security policies covering a range of topics. These policies are shared with and made available to all employees and contractors with access to WhosOnLocaiton information assets.

Training - All WhosOnLocation employees attend Security Awareness Training which is given within 14 days of hire and then on an annual basis. All developers undergo annual Secure Development Training on best practices and OWASP awareness.

Employee vetting

Background checks - WhosOnLocation performs background checks on all new employees in accordance with local laws. All contractors are required to complete a clean slate agreement and comply with our confidentiality agreements.

Confidentiality agreements - All employees and contractors are required to sign non-disclosure and confidentiality agreements.