



InteleGRID Security and Regulatory Overview

HIPAA

As a technology service provider, Intelemage is not a covered entity within the HIPAA guidelines. However, the system was designed and built in a way to help make certain that our clients and users can confidently use it knowing that they are meeting their HIPAA related obligations. The platform includes the following list of HIPAA compliance related checks and tools.

- a. All system use is fully audited
- b. All users are required to have their own unique logins
- c. All data transmissions and communications are encrypted
- d. All data traffic occurs over port 443 (SSL)
- e. Sessions timeout
- f. Users have access only to specific patient information that has been shared by another user with authority to do so
- g. All users are forced to electronically agree that they have read and understand their personal obligations related to HIPAA before using the inteleGRID

In accordance with the HITECH Act, Intelemage agrees to adhere to all regulations as set forth in order to appropriately and promptly notify both the customer and HHS as well as any other affected party of any security or PHI breach.

Regulatory

FDA Registration Information

Company Name:	Intelemage, LLC
FDA Owner/Operator #:	10026099
Medical Device Listing #:	D052892
Listing Status:	Active
Submission Type:	510(k) exempt
Product Code:	LMD
Classification:	892.2020 SYSTEM, DIGITAL IMAGE COMMUNICATIONS, RADIOLOGICAL

Proprietary Names: InteleGRID

Intelemage maintains a fully validated instance of the inteleGRID. The inteleGRID is currently supporting trials in over 30 countries worldwide. The solution complies with GCP and 21 CFR Part 11 guidelines.

Safe Harbor Certification

Certification Status: Current

Contact Office: Intelemage

Name: Chris Walsh , Director of Client Services

Phone: 877-464-7473

Fax: 513-352-9366

Email: cwalsh@intelemage.com

Original Certification: 9/19/2011

Next Certification: 9/19/2012

Privacy Policy Effective: 1/1/1900

Regulated By: Federal Trade Commission

Privacy Programs: NONE

Verification: In-House and Third Party Consultant

Security and Infrastructure

The Intelemage application and related infrastructure are exceptionally secure. We take multiple steps and we have made significant investments to ensure the protection of your data, including:

- a. Only outbound ports are used. No inbound data transmissions ever occur. Therefore, there is never a need to open your firewall for additional inbound ports

- b. Network Security: Multilayered defense through rich, integrated security services including stateful inspection firewalling, protocol and application inspection, in-line intrusion protection, and rich multimedia and voice security.
- c. Security Breach Monitoring & Notifications: Perimeter routers log all inbound/outbound traffic and notify the corporate IT security team of attempted security breaches.
- d. Encryption Model: SSL-based encryption methods are used on all communications with the inteleGRID.
- e. Data Center Security: Access is monitored 24/7, controlled by key fob access, and severely limited.
- f. Power Protection: All data center sites are connected to industry standard battery backup systems to provide clean power and protect against power loss. One of the data center sites also features a diesel generator that provides up to 36 hours of operation with onsite fuel.
- g. Fuel contracts are in place from multiple providers in the event of extended power downtime.
- h. Environmental Controls: The data center environments operated by Intelimage include first-class environmental controls to ensure continued and uninterrupted operation of the services provided by the inteleGRID. Controls include HVAC systems, water-free fire suppression, and environmental monitoring.
- i. Network Monitoring: All network devices and servers are monitored for availability, performance, and utilization. When a device fails or is not performing to the expected level, automatic notifications are sent out to the appropriate personnel.
- j. Bandwidth: Both Data Centers are equipped with over 100Mbps Internet access with the ability to scale to multi-Gigabit links.
- k. Redundancy and Data Center Sites (DR): The inteleGRID has been designed from the ground up for redundant operation. The inteleGRID Platform operates in an active-active mode across multiple data center sites for load balancing and disaster recovery purposes. All data is shared across multiple data centers in real time. The platform is supported by multiple redundant services from the data layer up. In addition to replication, data is backed up daily and archived to spinning disk for quick access.
- l. Bandwidth is monitored and automated reports are delivered to the network team daily.

Data Access Controls and Logical Separation of Data

Access to data:

Our system uses an LDAP directory for authentication and authorization. Users are authenticated against the directory which also defines their roles within the system. Additionally, users may be a part of a group and have roles within the group. Using these pieces of information the application restricts users to view data that has been specifically granted to a user or group of users with the proper roles associated. Access to data can be revoked in our

system and users can be removed or have their roles restricted to limit an individuals access to data.

Separation of data:

Image data is stored into separated directories based on the study instance UID, as dictated by the DICOM standard. This is relayed into our database structure and tied to the authorization framework to provide access on a study-by-study basis. Each study that our system maintains has its own position within our data structure including the case where the same study is received more than once (we keep a separate copy of each received study).

Encryption

Our system utilizes encryption for all communications outside of our internal data network. Images and data are transferred to and from the inteleGRID using our proprietary products to ensure data integrity, compression, and encryption. For data integrity our products calculate an MD5 checksum on each image prior to compression and transmission. Another MD5 checksum is calculated after the image is received and decompressed. The two checksum are verified to ensure the data received is the data sent. Our products only use loss-less compression to ensure the original image quality and integrity are met – this is matched up with the MD5 checksum to verify nothing has changed. Our client tools and products utilize Secure Sockets Layer (SSL) connections of 128-bit or greater encryption level. This is the same encryption your online bank and hundreds of thousands of other sites trust to secure their data during transmission.