

AG Mednet Meets Part 11 Compliance

Summary

AG Mednet, the world's largest diagnostic imaging exchange network, meets the requirements outlined by the Food and Drug Administration (FDA) in the application of Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures. Part of this white paper is based on the FDA's *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003/Pharmaceutical CGMPs)* and details how the AG Mednet image transfer platform:

- Addresses all FDA Part 11 compliance issues concerning electronic data transfer, security and audit trails.
- Provides a reliable, fast mechanism to securely and efficiently transmit studies.
- Offers several layers of protection, including those at the routing software level, to ensure that unauthorized data does not penetrate or traverse the network.
- Restricts portal access, as an extra security measure.

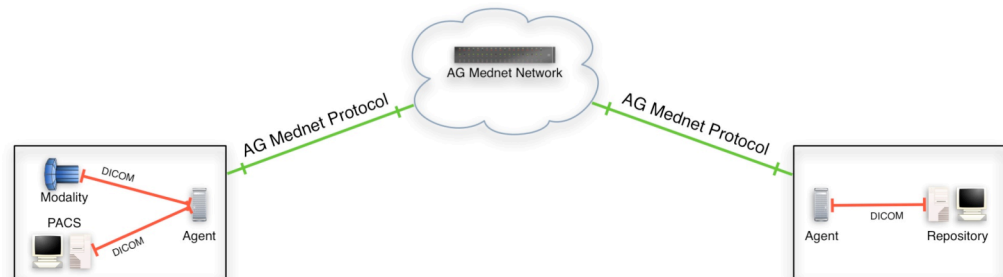
“Protecting and establishing accountability for image transfer is essential, and part of that responsibility is achieving Part 11 compliance,” explained Abraham Gutman, CEO for AG Mednet. “The AG Mednet image transfer platform provides the required technical controls to meet compliance by seamlessly addressing all issues concerning electronic data transfer, security and audit trails.”

Introduction

AG Mednet is a telecommunications network infrastructure dedicated exclusively to the transport of DICOM-based diagnostic image studies. Like other telecommunications networks, such as those operated by phone and cable companies, the AG Mednet image transfer platform receives data from systems on a LAN at the sending facility, and delivers it, through its private cloud, to another system residing on a LAN at a receiving site. AG Mednet does not enable users to directly see or modify any of the images as they are being moved: it simply provides a reliable, fast mechanism to effect transfers in a secure and efficient manner, maintaining bit-for-bit fidelity with the original copy of the study.

Network Elements and Security

AG Mednet consists of a leased fiber cloud on which resides its data centers, as well as devices at the edge called Agents. Agents on the network act as intelligent routers, capable of directing studies through the network to other destinations also subscribing to the AG Mednet network.



In March 1997, FDA issued final regulations (part 11) that provided criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, were intended to permit the widest possible use of electronic technology, consistent with FDA's responsibility to protect the public health.*

Network security being paramount, AG Mednet has implemented several layers of protection to ensure that unauthorized data does not penetrate or traverse the network. These layers include:

- **Access Control:** Agents at the edge of the network reside inside a site's firewall and also have their own active firewall. Agents accept traffic through a single port and respond to only well-formed DICOM protocol requests from known, registered devices on the LAN. All communications with the AG Mednet cloud are outbound and can only be initiated by the Agent. The Agent does not require, and will not respond to, any commands or queries originating anywhere, or from anyone, other than systems on the LAN, and only if they have been authorized to send through AG Mednet.

The AG Mednet network core residing at its data center is similarly protected. The core will only accept connections from registered Agents and only use proprietary AG Mednet protocols, which are unpublished. The AG Mednet core resides behind redundant firewalls—inside physically protected data centers with limited access using combinations of access cards and bio-metric access points. Within these data centers, servers are physically enclosed in cages with secret access codes.

- **Monitoring:** All elements of the AG Mednet network, both at the edge and at the core, are monitored 24/7/365, including intrusion attempts to its firewalls.

Routing Systems' Security and Logging

The aforementioned hardware elements run proprietary AG Mednet routing software, which is based on a subset of Linux. The Agent software is designed to interface with either DICOM-based devices on the edge. At the core, it is designed to interface only with AG Mednet Agents. Security at the routing software level is also paramount and includes:

- **Transient Nature of Data on the Network:** As AG Mednet is a transport network, its stated purpose is to securely receive, move and deliver data, after which the data is permanently removed from the network. AG Mednet retains imaging studies for seven days. This seven day period exists to ensure that if a recipient's network, or systems, is unavailable due to unforeseen circumstances, the sender can be assured that delivery of their traffic is pursued for at least one week.
- **Traffic Encryption:** When traffic begins to flow from an authorized system to an Agent, encryption of that traffic occurs prior to temporarily writing bits to the local hard drive. Traffic is securely encrypted: not generically, but specifically to the destination(s) where the sending system intends the traffic to be delivered. This provides a high level of security to ensure that in the unlikely event of a physical breach anywhere on the network, the data is protected from anyone that isn't the intended recipient, but who may also be on the network. Data on AG Mednet, whether at the core or on the edge, is always encrypted, and is decrypted only as part of the process of releasing it to the destination system.
- **Event Logging and Audit Trail:** As part of its routing process, software running the AG Mednet platform logs every event at each stage of the study transfer operation. The data captured by the logs is stored in a database that can be queried by an authorized member of the network operations team, and includes:
 - Sending system: name, brand, model number.

Since part 11 became effective in August 1997, significant discussions have ensued between industry, contractors and the agency concerning the interpretation and implementation of the rule. These concerns have been raised particularly in the areas of part 11 requirements for validation, audit trails, record retention, record copying and legacy systems.

- Study type: number of series, images, resolution.
 - Time stamps: date and time for each image transfer at each stage, including receipt from sending system, receipt from sending agent, receipt from core and acceptance by destination system.
 - Post-transfer additions: As the DICOM standard requires that individual images that were not part of the originally sent study, but are later sent, be accepted and made part of the original set, AG Mednet conforms to this requirement, while simultaneously logging the later additions. If any new images replace previously sent ones, the AG Mednet image transfer platform makes the old ones invisible, but does not delete them. New/invisible images are thoroughly logged.
- **Re-Routing:** AG Mednet provides a capability enabling authorized users to route studies that belong to them and are already on the network. In a clinical trial context, this situation may arise when one or more studies arrive at the central repository where, after a simple QA process, need to be further distributed for expert interpretation. If this occurs within the 7 day window, the recipient of the study can have access to a secure portal where, after entering their username and password, they can forward studies—where they are authorized to do so—directly from the core to specified addresses. When this happens, the aforementioned logging mechanism registers the transfer at each stage, including the username of the person affecting this transfer.

The FDA intends to enforce provisions related to:

- limiting system access to authorized individuals,
- use of operational system, authority and device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks,
- establishment of and adherence to written policies that hold individuals accountable,
- appropriate controls over systems documentation and open systems corresponding to controls for closed systems, and
- requirements related to electronic signatures

Portal Access

As previously mentioned, AG Mednet provides users with access to a network portal for reporting and routing purposes. It is important to note that through the portal, users do not have the capability of changing the content of the images, such as adding annotations or modifying the integrity of the original data. Access to the portal is restricted in two ways:

- **Each user must have a username and password to gain access.**
- Based on initial requirements specified when the user account is created, the user is restricted as to which specific studies/cases they are authorized to see (where “see” is strictly defined as “viewing a record specifying that said study/case has gone through the network”). Reasons for users to access the portal include:
 - **Routing:** An authorized user seeing that a study on the network is able to route this study to a location also on AG Mednet. The list of locations where this user is able to send studies is limited and defined when an AG Mednet administrator configures the individual user’s account.
 - **Transmittal Form:** Clinical trial cases are generally accompanied by a transmittal form completed by the sender. In the current courier-based system, these are sheets of paper placed into an envelope with the CD. A transmittal form is created by AG Mednet for each clinical trial that accomplishes two objectives:
 - **Parity:** As a physical shipment needs a transmittal form containing basic information, the electronic system provides a form that is linked to the case being sent. This form is different for every clinical trial. The fields in the form are completed by the sending facility and a record of its content, together with the name of the user and the

date/time it was completed, is logged for future audits. Once the form is completed by the sender, the fields can no longer be modified.

- **Permanent Linkage:** One of the shortcomings of paper/CD-based systems is that the link between the form and the images is tenuous, and depends on physical proximity. With the AG Mednet electronic form, cases and the information entered by the sender are linked, preventing the errors created when forms and cases are separated.

Compliance Summary

Requirement	How AG Mednet Achieves Compliance
<p style="text-align: center;">Validation</p> <p><i>Part 11 Section 11.10a</i> “Control for closed systems are to include the validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered records.”</p>	<p>Validation is achieved through the conjunction of two principles: data integrity and standards conformance.</p> <p>Data integrity is maintained through the use of encryption for the entire transmission set before any data is stored on the network. Any change to the encrypted data will render all the data un-decryptable, preventing unauthorized changes from being accepted by receiving systems.</p> <p>Standards conformance ensures that AG Mednet only accepts well formed DICOM transmissions. AG Mednet is exclusively a DICOM transport infrastructure and it strictly adheres to the standard (see AG Mednet DICOM Conformance Statement). This ensures that only DICOM studies sent by specifically authorized DICOM-compliant systems are accepted for transport on the network.</p>
<p style="text-align: center;">Audit Trail</p> <p><i>Part 11 Section 11.10(e)</i> “Audit trails must be secure, computer-generated and time-stamped to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. Audit trails should say 'who did what to your records and when.’”</p>	<p>All operations are logged and saved in a database for future reporting. Logged network information includes:</p> <ul style="list-style-type: none"> • Sending institution. • Sending modality/system. • Type and size of study/case: <ul style="list-style-type: none"> — Unique study ID. — Accession number. — Number of images. — Number of series. — Resolution parameters. • Time stamps: <ul style="list-style-type: none"> — Date. — Hour:minutes:seconds. <p>Logged user information includes:</p> <ul style="list-style-type: none"> • User name. • Time of login/logout. • Operations performed: <ul style="list-style-type: none"> — Forms filled. — Routing destination. — Time of routing initiation. <p>All image data on AG Mednet is transient and is deleted every 7 days. Transmission logs for all transfers on the network, including user routing operations, are securely and indefinitely kept for future audits.</p>
<p style="text-align: center;">Access Controls</p> <p><i>Part 11 Section 11.10(k)</i> “Use of secure, computer-generated, time-stamped audit trails to independently record and date the time of operator entries and actions that create, modify, or delete electronic records. 11.10(k)(2) covers the system documentation records regarding overall controls (such as access privilege logs, or system operational specification diagrams).”</p>	<p>The AG Mednet network and all of its components are closed systems. Data (cases) can flow into the Agents (edge devices) only if the sender systems (e.g., PACS, modalities, DICOM-conforming systems) are registered and known to the network. Agents can only transfer data to the network core if they are known, and have been authorized and authenticated by the core. Neither senders nor receivers of data login directly into Agents, which are computers without input devices (e.g. a keyboard, mouse or screen). Users view information on the network through a secure (login/encrypted password) system that enables them to look at certain traffic statistics (restricted in scope per user by a System Administrator) and allows them to route cases to a restricted set of destinations (restricted in scope per user by a System Administrator). Direct login to individual Agents and the network core is restricted to an AG Mednet System Administrator. In all cases, whether an AG Mednet System Administrator or a user viewing traffic, all operations are logged including username and time stamps for actions.</p>

About AG Mednet

AG Mednet is the world's largest diagnostic imaging exchange network. With AG Mednet, hospitals and diagnostic imaging centers provide the highest standard of scan interpretation to referring physicians, improving patient care and service. Radiologists who want to expand their business benefit from anytime/anywhere access to flawless images. Pharmaceutical, bio-tech, device and clinical research organizations that utilize imaging technology now have an automated way to recruit imaging sites and exchange secure images, reducing time and costs. AG Mednet is headquartered in Boston and serves the global medical community. For more information call 1-888-9AGMEDNET or visit www.agmednet.com.

* FDA, *Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application*, 8/28/03, <http://www.fda.gov/cder/guidance/5667fnl.pdf>