
Rev 3

Novarad Corporation is dedicated to helping our customers ensure the confidentiality, integrity and availability of their electronic health information. Novarad makes every effort to conduct our business in compliance with the privacy and security standards set forth in the Health Insurance Portability and Accountability (HIPAA) Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) ACT of 2009, and all other applicable information security standards as required by law.

Although Novarad is committed to ensuring the privacy and security of customer information accessible at our site and provides tools in our software solutions to help our customers implement privacy and security standards in their own facilities, it is ultimately the responsibility of individual healthcare providers to maintain HIPAA/HITECH compliance and ensure the privacy and security of Protected Health Information (PHI) for their establishment. Novarad's responsibilities for ensuring the privacy and security of customer information are outlined in our Business Associate Agreement.

Note: For more information on HIPAA/HITECH, please refer to information provided by the US Department of Health and Human Services: <http://www.hhs.gov/ocr/privacy/>.

The following sections outline some of the privacy and security measures taken by Novarad and available in our software solutions to help customers protect their electronic information:

A. Novarad Corporate Operational Procedures

Novarad has internal policies and procedures in place to ensure information security. The following sections outline some of these measures:

1. Building Security and Access

Novarad has a full building security system that limits access to approved Novarad employees and visitors. This helps ensure the physical security of all PHI stored onsite. Additional security measures are taken at the physical storage location of customer information (on- and offsite) to further limit access to the appropriate personnel.

2. Network Security and Access

All Novarad employees have their own private login for network access. Network access for individual employees is limited to only the PHI needed to complete their job functions.

3. Employee Confidentiality and Training

All Novarad employees sign confidentiality agreements and complete HIPAA training as a condition of employment. This agreement prohibits the employee

Rev 3

from divulging PHI according to the rules of HIPAA. It is against Novarad corporate policy for Novarad employees to transmit or duplicate PHI that contains identifying information to a 3rd party.

4. Customer Agreements

Novarad customers are required to execute a standard sales agreement. In turn, Novarad and its customers also execute a Business Associate Agreement (BAA) that sets forth the specific responsibilities of the customer and Novarad.

5. Business Continuity and Disaster Recovery

Novarad has policies for responding to an emergency or other occurrence (e.g. fire, vandalism, system failure, and natural disaster) that damages systems. The contingency plan applies to the functions, operations, and resources necessary to restore and resume Novarad's system operations. Annual reviews of the facility disaster recovery/contingency plans are in place.

B. Software Solutions

All Novarad Products are designed and developed in compliance with all applicable regulatory requirements and with Information security in mind. The following sections outline some of the features available in our products to help ensure information security:

Offsite Image Archive Service

Below is a list of some of the ways Novarad protects PHI in the context of our Offsite Image Archive service:

- PHI backed up to Novarad via the Internet uses 128-bit or better encryption.
- There are firewalls protecting the systems from inappropriate access.
- Physical access to the server is limited to the IT department.
- Images are backed up onto two different servers, one offsite in case of network failure, fire, etc.
- Escalation and IT are the only departments with access to server data.

NovaPACS/RIS Features That Aid HIPAA Compliance

This section discusses features of the NovaPACS/RIS systems that aid customers in maintaining HIPAA compliance in their facilities.

Rev 3

Authentication

- NovaPACS/RIS Systems are configured to require users to log on before they are able to access PHI.

Access Control

- Novarad policy is to give each user a unique username and password. We do not advise or support password sharing.
- NovaPACS/RIS supports restricting a user's access to only certain patient data.
- NovaPACS/RIS supports automatically "logging off" users if a workstation goes unused for a period of time.
- Novarad assists customers in choosing secure areas in which to place equipment, where appropriate.
- NovaPACS/RIS allow limited access to patient data and images based on clinical role.

Auditing

- NovaPACS/RIS maintains a log of users' access to patient information. Administrators may review this log from time to time to verify that information is being accessed appropriately.

Data Integrity

- Data is stored on fault-tolerant systems.
- NovaPACS/RIS has redundant server capability for easy failover to prevent down-time.
- NovaPACS/RIS supports backing up data offsite for disaster recovery purposes.

Transmission Security

- Data transmissions via Internet are encrypted with 128-bit or better encryption technology such as SSL or VPN.
 - Novarad supports the display of a post-login message warning the user about the confidentiality of the information about to be viewed.
-

Novarad Contact Information

752 E. 1180 S • American, Fork, UT 84003 • FAX: (801) 642-1030

Technical Support

Phone: (801) 221-5895

E-Mail: service@novapacs.com

Sales

Phone: (877) Novarad (877-668-2723)

E-Mail: sales@novapacs.com