HIPAA COMPLIANCE STATEMENT

Merge Healthcare
900 Walnut Ridge Drive
Hartland, WI 53029
**INDICATIONS FOR USE: Merge Unity PACS**

Merge Unity PACS is a medical image and information management system that allows viewing, selection, processing, printing, telecommunications, and media interchange of medical images from a variety of diagnostic imaging systems. Merge Unity PACS interfaces to various storage and printing devices using DICOM or similar interface standards. Merge Unity PACS displays, stores, prints, and telecommunicates images from a number of medical modalities, including but not limited to MRI, CT, US, PET, DXA (bone densitometry), nuclear imaging, computed radiography, digital radiography, digitized films, digital photographs, mammographic images, and processed data from FDA-cleared third party image processing systems, including FDA-cleared systems for computer-aided detection and advanced image processing (e.g. 3-D processed images such as those produced by Voxar Corp.).

Lossy compressed mammographic images must not be used for primary diagnostic interpretation unless approved for use in digital mammography. Display monitors used for primary diagnostic interpretation of mammographic images must be approved for use in digital mammography.

**INDICATIONS FOR USE: Z3D**

Z3D is intended to provide reading physicians, referring physicians, and other appropriate healthcare professionals tools to aid in interpreting medical images, including:

- Displaying DICOM compliant medical image volumes, such as CT, MRI, and PET.
- Reformatting images, including creation of MPRs, MIPs, MiniIPs, color/monochrome 3D volume rendered images.
- Manipulating displayed images via control of slice thickness, slice interval, obliquity, perspective, rotation, window/level, crop, zoom, color/monochrome transformations, segmentation, sculpting, straightening the display of curved structures, and creating images perpendicular to a curvilinear path.
- Creating series of DICOM images and individually captured images that can be displayed and stored in a PACS.
- Measuring coronary calcium, which is intended for non-invasive identification and quantification of calcified atherosclerotic plaques in the coronary arteries using tomographic medical image data and clinically accepted calcium scoring algorithms.

**CAUTION:** Federal law restricts this device to sale by or on the order of a physician.

**CAUTION:** Unity PACS and Merge Z3D are not intended for diagnostic use on mobile device such as a phone or tablet.


**CANADIAN DEVICE IDENTIFIER:**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNITY RIS/PACS</td>
<td>C-DRSW-00001</td>
</tr>
<tr>
<td>Merge Z3D</td>
<td>MERGE Z3D</td>
</tr>
</tbody>
</table>

Manufacturer’s Address
Merge Healthcare Incorporated
900 Walnut Ridge Drive
Hartland, WI 53029
### DOCUMENT VERSION LOG:

<table>
<thead>
<tr>
<th>Part</th>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPAX-4462</td>
<td>June 7, 2016</td>
<td>1</td>
<td>Initial Merge release.</td>
</tr>
<tr>
<td></td>
<td>May 10, 2017</td>
<td>2</td>
<td>Updated copyright page and migrated to Merge template.</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction .............................................................................................................................. 5
   1.1 Purpose ................................................................................................................................ 5
   1.2 Scope ..................................................................................................................................... 5
   1.3 Related Information .............................................................................................................. 5
   1.4 Glossary ............................................................................................................................... 6

2. Responsibility for compliance ............................................................................................. 6

3. How DR Systems supports compliance internally .......................................................... 6

4. How DR Systems supports compliance for its customers ............................................ 7
   4.1 Access controls ..................................................................................................................... 7
   4.2 Audit controls ....................................................................................................................... 8
   4.3 Integrity ............................................................................................................................... 8
   4.4 Authentication .................................................................................................................... 8
   4.5 Transmission security .......................................................................................................... 8
1 Introduction

1.1 Purpose

The purpose of this document is to provide general information in relationship to the technical security services referenced within the Technical Safeguards section of the Federal Register, Section G (164.312), as they pertain to Protected Health Information in electronic form.

DR Systems’ products are designed to assure the privacy and security of electronically stored medical data. The regulations set standards for electronic transactions, the privacy of all medical records and all identifiable health information and the security of electronically stored information. DR Systems’ products are designed to assist Covered Entities (as defined under HIPAA) to comply with the HIPAA Regulations referenced in this document.

1.2 Scope

The scope of this document is focused solely on the five technical security services requirements with supporting implementation features: Access control; Audit Controls; Integrity; Person or Entity authentication; and Transmission Security. For details, reference Technical Safeguards section of the Federal Register, Section G (164.312).

All other required privacy and security elements associated with the HIPAA regulations are the sole responsibility of the Covered Entities. Note: a complete description of HIPAA is beyond the scope of this document.

1.3 Related Information

The following are Web sites with related information:

<table>
<thead>
<tr>
<th>Web Site</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.hhs.gov/ocr/hipaa/">http://www.hhs.gov/ocr/hipaa/</a></td>
<td>United States Department of Health and Human Services</td>
</tr>
<tr>
<td></td>
<td>Office for Civil Rights - HIPAA</td>
</tr>
<tr>
<td></td>
<td>Medical Privacy – National Standards To Protect the Privacy of Personal Health Information</td>
</tr>
<tr>
<td><a href="http://ecfr.gpoaccess.gov/cgi/t/text-idx?c=ecfr&amp;tpl=/ecfrbrowse/Title45/45cfr162_main_02.tpl">http://ecfr.gpoaccess.gov/cgi/t/text-idx?c=ecfr&amp;tpl=/ecfrbrowse/Title45/45cfr162_main_02.tpl</a></td>
<td></td>
</tr>
</tbody>
</table>
1.4 Glossary

Business Associate

Under HIPAA, “Business Associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information, on behalf of, or provides service to, covered entity.

Covered Entity (CE)

Under HIPAA, “Covered Entity” is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. Also see Part II, 45 CFR 160.103.

HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates legal and regulatory environments governing the provision of health benefits, the delivery and payment of healthcare services, and the security and confidentiality of individually identifiable, protected health information.

Protected Health Information (PHI)

PHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. See Part II, 45 CFR 164.501

2 Responsibility for compliance

Compliance with state and federal regulations regarding patient confidentiality, security, and privacy is the responsibility of all covered entities and business associates. This includes, but is not limited to, compliance with the Health Information Portability and Accountability Act (HIPAA) of 1996.

3 How DR Systems supports compliance internally

DR Systems supports compliance with regulatory and ethical requirements in many ways:

1. Confidentiality agreement. All DR employees are required to execute a confidentiality agreement, because employees may gain access to confidential medical information as a result
of their work with clinical customer sites. A copy of DR Systems’ internal confidentiality agreement can be provided upon request.

2. **Background checks before hiring.** A background check is performed on all new hires to DR Systems.

3. **Requirement for creating anonymized patient records.** DR Systems’ internal policies prohibit the inappropriate transmission or duplication of patient records, if the patient records include identifying information.

### 4 How DR Systems supports compliance for its customers

In the Technical Safeguards section of the Federal Register, Section G (164.312), the following security services features are discussed:

- Access Controls
- Audit Controls
- Integrity
- Authentication
- Transmission Security

See the following sections for details on how DR Systems addresses these features.

#### 4.1 Access controls

Requirements for unique user identification and other methods of access control:

- **Unique user identification.** DR Systems supports a username/password system for gaining access to DR Systems user applications. We strongly discourage any user from sharing or disclosing this personal password or user name.

- **Restrictions based on user rights.** User Security Administration enables certain Administrators to tailor the rights assigned to any given user, including limiting and suspending user rights as appropriate.

- **Automated log-outs.** DR Systems supports an automatic logout mechanism. The system requires the user to log on again, if the workstation is not used for a selected period of time.

- **Placement of equipment in secure areas.** DR Systems participates with customers in planning implementation so that confidentiality and security is promoted. This includes placing computer technology in appropriately secured and confidential areas when applicable.
4.2 Audit controls

Audit control procedures to record and examine system activity:

- **Audit trail.** DR Systems provides an audit trail that records access to any patient’s medical record within DR Systems’ products. The event log can be queried and sorted, and can also be copied to external databases such as Microsoft Excel.

4.3 Integrity

Integrity is maintained through the following methods:

- **Archiving and backup methods.** DR Systems provides a multi-tiered archive to ensure security of imaging and related records. DR Systems strongly encourages all customers to create backup copies of their medical imaging records using our Archiving systems when applicable.
- **Disaster planning support.** DR Systems’ supplies fault-tolerant image servers and other related technologies to support disaster planning when necessary. For example, technologist workstations can be configured to continue functioning even in the event of a server or network failure, so that patient imaging can continue. Patient demographics and exam schedules can be input directly into DR Systems in the event of a particular failure.

4.4 Authentication

- **User Authentication** – Username/password system.
- **Approval and authentication of reports.** Some of DR products’ supports approval and authentication of reports, which can include electronic signature. User names and passwords are required to generate, edit, revise, or correct reports and appropriate audit trails are retained.

4.5 Transmission security

- **Data encryption.** The system supports data encryption when information is transmitted via the Internet, using secure technology such as SSL, TLS, or VPN.
- **Confidentiality warning.** Appropriate confidentiality notices are displayed when records are queried over the Internet.