AGFA HealthCare	**Document Number**: *40052412*
	This information is Company Confidential

Manufacturer Disclosure Statement for Medical Device Security

IMPAX Agility
(IMPAX Next Generation)
(P/07681)

Owner/Responsible	
Program Manager	Nadia De Paepe

Key Author(s)	
Program Manager	Nadia De Paepe

Review/ToBeConsulted	
Solution Manager	Joost Felix
Solution Architect	Nikolas Boel
QARA Representative	Jodi Coleman
Global ISP Manager	Geert Claeys

Approval/Accountable	
Global ISP Manager	Geert Claeys
QARA Representative	Jodi Coleman
Program Manager	Nadia De Paepe
Solution Manager	Joost Felix

Remove this front page when, after approval, prior to distribution externally to Agfa HealthCare

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

IMPAX Agility

Version 1.x
March 26, 2013

Issued by:
Agfa HealthCare
Septestraat 27
B-2640 Mortsel
Belgium

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

The National Electrical Manufacturers Association (NEMA) standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEITHER HEALTH INFORMATION MANAGEMENT SYSTEMS SOCIETY (HIMSS) NOR NEMA HAVE POWER, NOR DO THEY UNDERTAKE TO POLICE OR ENFORCE COMPLIANCE WITH THE CONTENTS OF THIS DOCUMENT. NEITHER HIMSS NOR NEMA CERTIFY, TEST, OR INSPECT PRODUCTS, DESIGNS, OR INSTALLATIONS FOR SAFETY OR HEALTH PURPOSES. ANY CERTIFICATION OR OTHER STATEMENT OF COMPLIANCE WITH ANY HEALTH OR SAFETY–RELATED INFORMATION IN THIS DOCUMENT SHALL NOT BE ATTRIBUTABLE TO HIMSS OR NEMA AND IS SOLELY THE RESPONSIBILITY OF THE CERTIFIER OR MAKER OF THE STATEMENT.

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

FOREWORD

This document consists of the Manufacturer Disclosure Statement for Medical Device Security (MDS^2 form). The intent of the MDS^2 form is to supply healthcare providers with important information to assist them in assessing the VULNERABILITY and risks associated with protecting ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) transmitted or maintained by medical devices. Because security risk assessment spans an entire organization, this document focuses on only those elements of the security risk assessment process associated with medical devices and systems that maintain or transmit ePHI.

The MDS^2 form should:

(1) Be useful to healthcare provider organizations worldwide. While the form does supply information important to providers who must comply with HIPAA privacy and security rules, the information presented may be useful for any healthcare provider who aspires to have an effective information security RISK MANAGEMENT program. Outside the US, providers would therefore find the MDS^2 form an effective tool to address regional regulations such as EU 95/46 (Europe), Act on the Protection of Personal Information (Act No. 57 of 2003, Japan), and PIPEDA (Canada).

(2) Include device specific information addressing the technical security-related attributes of the individual device model.

(3) Provide a simple, flexible way of collecting the technical, device-specific elements of the common/typical information needed by provider organizations (device users/operators) to begin medical device information security (i.e., confidentiality, integrity, availability) risk assessments.

(4) HIMSS and NEMA grant permission to make copies and use this form.

Using the information in the MDS^2 form together with information collected about the care delivery environment (e.g., through tools like ACCE / ECRI's Guide for Information Security for Biomedical Technology), the provider's multidisciplinary risk assessment team can review assembled information and make informed decisions on implementing a local security management plan.

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Section 1
INSTRUCTIONS FOR OBTAINING AND USING THE MDS^2 FORM

1.1 OBTAINING THE MDS^2 FORM (HEALTHCARE PROVIDERS)

Completed MDS^2 forms for many devices and systems may be available directly from the Agfa HealthCare Product Security Website: http://www.agfa.com/main/productsecurity/mds2/ .

1.2 USING THE MDS^2 FORM (HEALTHCARE PROVIDERS)

1.2.1 Section 1 – Questions 1-19

Section 1 of the MDS^2 form contains information on the type of data maintained / transmitted by the device, how the data is maintained / transmitted, and other security-related features incorporated in the device, as appropriate. The field "Other Security Considerations" allows the manufacturer to add some general security considerations.

PLEASE BE ADVISED—An indication of a device's ability to perform any listed function (i.e., a "Yes" answer) is not an implicit or explicit endorsement or authorization by the manufacturer to configure the device or cause the device to perform those listed functions.

It is important to distinguish between capability and permission. The questions contained on the MDS^2 form refer to device capability. Permission is a contractual matter separate from the MDS^2 form and is not covered by the MDS^2 form. Making changes to a device without explicit manufacturer authorization may have significant contractual and liability issues.

1.2.2 Section 2 – Explanatory notes

The optional section 2 of the MDS^2 form contains space for explanatory notes if the manufacturer needs more space to explain specific details to the answers on questions 1-19. .

NOTE—Agfa HealthCare may elect to attach supplementary material if additional space for recommended practices or explanatory notes is necessary.

1.3 THE ROLE OF HEALTHCARE PROVIDERS IN THE SECURITY MANAGEMENT PROCESS

The healthcare provider organization (e.g. a hospital) has the ultimate responsibility for providing effective security management. Agfa HealtCare can assist providers in their security management programs by offering information describing:

- the type of data maintained / transmitted by the Agfa HealtCare's device or system;
- how data is maintained / transmitted by the Agfa HealtCare's device or system;
- any security–related features incorporated in the Agfa HealtCare's device or system.

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

In order to effectively manage medical information security and comply with relevant regulations, healthcare providers must employ ADMINISTRATIVE, PHYSICAL and TECHNICAL SAFEGUARDS—most of which are extrinsic to the actual device

1.4 DEFINITIONS

Administrative Safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ELECTRONIC PROTECTED HEALTH INFORMATION and to manage the conduct of the covered entity's workforce in relation to the protection of that information. [45 CFR Part 164]

Anti-Virus Software: See VIRUS SCANNER

Audit trail: Data collected and potentially used to facilitate a security audit [45 CFR Part 142]

Biometric ID: A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, handwritten signature). [45 CFR Part 142]

Electronic Media: (1) Electronic storage media, including memory devices in computers (hard drives) and any removable/transportable digital memory media, such as magnetic tapes or disks, optical disks, or digital memory cards. (2) Transmission media used to exchange information already in electronic storage media, including, for example, the Internet (wide open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, and private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile and of voice via telephone, are not considered to be transmissions via ELECTRONIC MEDIA because the information being exchanged did not exist in electronic form before the transmission. [45 CFR Part 160.103]

Electronic Protected Health Information (ePHI): INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI) that is (1) transmitted by or (2) maintained in ELECTRONIC MEDIA. [45 CFR Part 160.103]

Individually Identifiable Health Information (IIHI): INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. [45 CFR Part 160.103].

Personal Identification Number (PIN): A number or code assigned to an individual and used to provide verification of identity. [45 CFR Part 142]

Physical Safeguards: The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. [45 CFR Part 164]

Remote Service: A support service (e.g., testing, diagnostics, software upgrades) while not physically or directly connected to the device (e.g., remote access via modem, network, Internet).

Removable Media: See ELECTRONIC MEDIA

Risk Analysis: Conducting an accurate and thorough assessment of the potential risks and VULNERABILITIES to the integrity, availability, and confidentiality of ELECTRONIC PROTECTED HEALTH INFORMATION. [45 CFR Part 164]

Risk Management: (1) The ongoing process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. [NIST SP 800-26] (2) Security measures sufficient to reduce risks and VULNERABILITIES to a reasonable and appropriate level. [45 CFR Part 164]

Technical Safeguards: The technology, policies, and procedures to protect ELECTRONIC PROTECTED HEALTH INFORMATION and control access to it. [45 CFR Part 164]

Token: A physical authentication device that the user carries (e.g., smartcard, SecureID^{tm}, etc.). Often combined with a PIN to provide a two-factor authentication method that is generally thought of as superior to simple password authentication.

Virus: In general, computer code that is either:

(1) A type of programmed threat—a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

(2) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs; in addition to propagation, the VIRUS usually performs some unwanted function. [45 CFR Part 164]

Virus scanner: A computer program ("ANTI-VIRUS SOFTWARE") that detects a VIRUS computer program, or other kind of malware (e.g., worms and Trojans), warns of its presence, and attempts to prevent it from affecting the protected computer. Malware often results in undesired side effects generally unanticipated by the user.)

Vulnerability: A flaw or weakness in system procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [NIST SP 800-30]

ARCRONYMS

CD: Compact Disk

CF: Compact Flash

DVD:	Digital Versatile Disk
IP:	Internet Protocol
LAN:	Local Area Network
ROM:	Read Only Memory
SD:	Secure Digital
USB:	Universal Serial Bus
VPN:	Virtual Private Network
WAN:	Wide Area Network
WiFi:	Wireless Fidelity

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Section 2
MDS^2 FORM

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	*Agfa HealthCare*	*40052412*	*March 2013*
Device Model	**Software Revision**	**Software Release Date**	
IMPAX Agility	*1.x*	*March 2013*	

Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information
	Agfa HealthCare	*Agfa HealthCare N.V*
	Representative Name/ Position	*Septestraat 27*
	Global ISP manager – Agfa Healthcare	*B-2640 Mortsel, Belgium*
		Tel. +32 3 444 2111

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	Yes No N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?	Yes	
2. Types of ePHI data elements that can be maintained by the device:		
a. Demographic (e.g., name, address, location, unique identification number)?	Yes	
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	Yes	
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	
d. Open, unstructured text entered by device user/operator?	Yes	
3. Maintaining ePHI - Can the device		
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?	Yes	
b. Store ePHI persistently on local media?	Yes	
c. Import/export ePHI with other systems?	Yes	
4. Mechanisms used for the transmitting, importing/exporting of ePHI – Can the device		
a. Display ePHI (e.g., video display)?	Yes	
b. Generate hardcopy reports or images containing ePHI?	Yes	
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?	Yes	
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	Yes	
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?	Yes	1
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?	Yes	2
g. Other?_____	No	

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	Yes	
6. What underlying operating system(s) (including version number) are used by the device? _	Windows	
Application Server : Windows Server 2008 R2, 64 bit only		
Client: Windows 7 (32/64bit), Vista (32/64bit). Radiologist desktop runs on Windows 7 – 64 bit		

PHYSICAL SAFEGUARDS	Yes No N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e. cannot remove without tools)?	Yes	
8. Does the device have an integral data backup capability (i.e., backup onto removable media like tape, disk)?	Yes	
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No	

DOCUMENT CONTROL NOTE:

AGFA HealthCare

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	*Agfa HealthCare*	*40052412*	*March 2013*

Device Model	Software Revision	Software Release Date
IMPAX Agility	*1.x*	*March 2013*

Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information
	Agfa HealthCare	*Agfa HealthCare N.V*
	Representative Name/ Position	*Septestraat 27*
	Global ISP manager – Agfa Healthcare	*B-2640 Mortsel, Belgium*
		Tel. +32 3 444 2111

TECHNICAL SAFEGUARDS	Yes No N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	Yes	3
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?	Yes	
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	Yes	
b. Can the device provide an audit trail of remote-service activity?	Yes	
c. Can security patches or other software be installed remotely?	Yes	
12. Level of owner/operator service access to device operating system: Can the device owner/operator		
a. Apply device manufacturer-validated security patches?	Yes	
b. Install or update antivirus software?	Yes	
c. Update virus definitions on manufacturer-installed antivirus software?	Yes	
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?	Yes	
13. Does the device support user/operator specific username *and* password.	Yes	
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock).	Yes	
15. Events recorded in device audit trail (e.g., user, date/time, action taken): Can the audit trail record		
a. Login and logout by users/operators?	Yes	
b. Viewing of ePHI?	Yes	
c. Creation, modification or deletion of ePHI?	Yes	
d. Import/export or transmittal/receipt of ePHI?	Yes	
16. Does the device incorporate an emergency access ("break-glass") feature that is logged?	Yes	
17. Can the device maintain ePHI during power service interruptions?	Yes	
18. Controls when exchanging ePHI with other devices:		
a. Transmitted only via a point-to-point dedicated cable?	Yes	4
b. Encrypted prior to transmission via a network or removable media?	Yes	5
c. Restricted to a fixed list of network destinations	Yes	6
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?	Yes	

DOCUMENT CONTROL NOTE:

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	*Agfa HealthCare*	*40052412*	*March 2013*

Device Model	Software Revision	Software Release Date
IMPAX Agility	*1.x*	*March 2013*

Manufacturer or Representative Contact Information:	Company Name	Manufacturer Contact Information
	Agfa HealthCare	*Agfa HealthCare N.V*
	Representative Name/ Position	*Septestraat 27*
	Global ISP manager – Agfa Healthcare	*B-2640 Mortsel, Belgium*
		Tel. +32 3 444 2111

Other Security Considerations

Authentication

A token based authentication system, built on the JAAS standard (Java Authentication and Authorization Service) is available. On initial login, users are required to enter username/password. These credentials are used to retrieve a token from the Agility authentication service. A token identifies a user session, has a limited lifetime and must be used for all subsequent server calls. It can validate credentials against various sources (e.g. Agility DB, external LDAP …) by configuring the appropriate login modules. When the user fails to correctly authenticate 3 times the account of the user is locked for a period of time. A strong password policy can be enforced.

Access Control

The impact of authorization is two-fold:

- It limits what a user can do; for example a user can only create an addendum on a report if he is the author of the original report.
- It limits what a user can see; for example a user can only see patient details for patients located in his department.

IMPAX Agility supports a "break the glass – emergency access" feature, if configured as part of the security role of the user. The user has the ability to break the by security enforced access control to what study data he can "see". The "break the glass - emergency access" feature is an audited feature which allows the user to expand the normal defined query results for emergency cases.

Auditing

IMPAX Agility has the concept of task history, utilizing the task history you can check who has performed which action in which point in time. Additionally IMPAX Agility can be configured to send out audit messaging towards an external Audit Record Repository. It follows the IHE ATNA specification regarding the timing and content of the audit messages that it produces and is HIPAA (Health Insurance Portability and Accountability Act) compliant.

System Hardening

The IMPAX Agility Installer will enable the Windows firewall if not already enabled, registering exceptions for the ports required to run the Application Server. The Windows firewall will not allow external connections to any other ports. The IMPAX Agility installer will also disable

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	*Agfa HealthCare*	*40052412*	*March 2013*
Device Model	**Software Revision**	**Software Release Date**	
IMPAX Agility	*1.x*	*March 2013*	

Manufacturer or Representative Contact Information:	Company Name *Agfa HealthCare*	Manufacturer Contact Information *Agfa HealthCare N.V*
	Representative Name/ Position *Global ISP manager – Agfa Healthcare*	*Septestraat 27* *B-2640 Mortsel, Belgium* *Tel. +32 3 444 2111*

some default Windows services that not required to run the Application Server and/or are linked to known security vulnerabilities.

Code Signing and Obfuscation

The Web Application downloadable components are signed with an Agfa Healthcare private code signing certificate. The client's netboot process responsible to launch the IMPAX Agility clients enforces all plugins of the client to be signed. The client doesn't start when not all plugins are signed by the Agfa Healthcare private code signing certificate. Some parts of the code (eg. Licensing, authentication, access control …) are obfuscated,

Encryption

For communication with external systems including the IMPAX Agility client and Xero Web Viewer, IMPAX Agility uses SSL (specifically TLS) secure communication. The encryption algorithm is specified by the certificates in use, and implemented by the SSL socket layer.

Licensing

The Agility licensing system supports two types of licenses:

- Concurrent licenses, where multiple users can concurrently use a feature. The number of concurrent users is determined by the allowed number of concurrent licenses.
- Volume licenses, where a feature can only be used for a certain number of times. This number is defined in the license.

SECTION 2

Product Name
Version 1.x

Manufacturer Disclosure Statement for Medical Device Security

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Medical Device Software	*Agfa HealthCare*	*40052412*	*March 2013*
Device Model	**Software Revision**	**Software Release Date**	
IMPAX Agility	*1.x*	*March 2013*	

Manufacturer or Representative Contact Information:	Company Name *Agfa HealthCare*	Manufacturer Contact Information *Agfa HealthCare N.V* *Septestraat 27* *B-2640 Mortsel, Belgium* *Tel. +32 3 444 2111*
	Representative Name/ Position *Global ISP manager – Agfa Healthcare*	

EXPLANATORY NOTES (from questions 1 – 19)
IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form).

1. Communication only happens using secure communication lines
2. Communication between IMPAX Agility Client & Server can be wireless Receiving and transmitting data wirelessly is possible if enabled by the hardware… however, it is not a standard configuration
3. Extra software can be installed on client workstations. No other software is allowed to be installed on servers.
4. Paper rinting
5. HTTPS communication
6. List is restricted to defined external systems

Details as of PDF Creation Date

Document Metadata

Title:	Manufacturer Disclosure Statement IMPAX Agility.doc
Livelink ID:	40052412
Version#:	4
Version Date:	2013/03/22 06:32 PM CET
Status:	Approved on 2013/03/26 03:48 AM CET
Owner:	Nadia De Paepe (amiqb)
Created By:	Nadia De Paepe (amiqb)
Created Date:	2013/03/18 01:36 PM CET
PDF Creation Date:	2013/03/26 03:48 AM CET

This document was approved by:

Signatures:

1. Joost Felix (abjfx) on 2013/03/26 03:04 AM CET
2. Geert Claeys (amclg) on 2013/03/25 05:03 PM CET
3. Nadia De Paepe (amiqb) on 2013/03/22 06:40 PM CET
4. Jodi Coleman (axkcg) on 2013/03/22 08:02 PM CET

Detailed Approver History:

- **Approval Workflow started on 2013/03/22 06:38 PM CET**
  - Approval task originally assigned to and completed by Nadia De Paepe (amiqb) on 2013/03/22 06:40 PM CET
  - Approval task originally assigned to and completed by Jodi Coleman (axkcg) on 2013/03/22 08:02 PM CET
  - Approval task originally assigned to and completed by Joost Felix (abjfx) on 2013/03/26 03:04 AM CET
  - Approval task originally assigned to and completed by Geert Claeys (amclg) on 2013/03/25 05:03 PM CET

Version & Status History

Version#	Date Created	Status
4	2013/03/22 06:32 PM CET	Approved - 2013/03/26
3	2013/03/18 01:40 PM CET	Reviewed - 2013/03/22

2	2013/03/18 01:37 PM CET	
1	2013/03/18 01:36 PM CET	