PHILIPS HEALTHCARE

Trainee Name:	
Trainee Signature:	
Date:	

Course Title	Local Course Code	Revision
Customer Service Media Disposition Procedure	5104-0370	C

By submitting this form, I agree that I have completed the required training for this course and understand the material and the impact on my job responsibility.

Signed by 3rd Party Contractor Training Representative:

_____ Date: _____

This form is to be kept as a formal training record by the 3rd Party Contractor Agency

PHILIPS PHNA

Document Number: **5104-0370 C**

Title: **Customer Services Media Disposition Procedure**

Effective Date: **See PDM**

Approvals:	**Title**	**Name**	**Date**
Process Owner:	Sr Manager, Project-Client Service	Bill Stewart	See PDM
Designated User(s):	Vice President, Imaging Systems	Robert Stevens	See PDM
	Senior Director, Field Service	Jon Fazekas	See PDM
	Senior Director, PCMS Zone Service	Christopher La Fratta	See PDM

Note: The Process Owner and Designated User names are here for reference only and may not be current. See PDM for the current Process Owner and Designated User names.

Rev	Major / Minor	Description
C	Major	Add "Appendix C" – default media handling guidelines for Businesses without an existing / adequate guideline / process Add "Appendix D" – procedure for local media destruction when customers refuse to accept possession of old/un-needed media
B	Major	Add media sanitization and encryption options / alternatives.
A		Initial release.

1.0 PURPOSE AND SCOPE

The purpose of this policy is to guide the field service organization in the handling of Storage Media such as hard drives, CD/DVD Media or any other storage Media utilized in Philips Healthcare products. In order to be compliant with Philips Healthcare Privacy Policy and PHNA Protected Health Information Policy, Philips Healthcare is required to limit access to and prevent unauthorized disclosure of Personal Data. When Storage Media needs to be replaced or removed from Philips systems during the provision of service, this is accomplished primarily by minimizing the handling of used Storage Media and, whenever feasible, Encrypting or Sanitizing the media or simply leaving the Storage Media in the Customer's control as described in the subsequent sections.

1.1. In Scope

This procedure is applicable to all Philips Customer Services employees within Philips Health Systems, North American Market (PHNA) and all Distributor and third party service personnel performing service in the name of Philips Healthcare. It applies to all situations where systems or parts that contain Storage Media are being replaced or removed by Philips from a Philips Healthcare product during the provision of service. This policy outlines the expected behavior and processes to follow with respect to Storage Media handling. It applies to any Storage Media that has been used, even if only on a temporary basis, in or with a Philips Healthcare product.

1.2. Out of scope

This procedure does NOT cover the handling of Storage Media used for the gathering of information for clinical trials, clinical demonstrations, research and other situations where a separate written agreement with the Customer exists - including sales loaner systems, sales demo systems or trade-ins.
Philips approved and issued service tools such as Field Service Engineer (FSE) laptops and other service tools provided by Philips are also outside the scope of this procedure.

2.0 EXPLANATION OF KEY TERMS

AoMD -	(Philips Healthcare) Authorization of Media Disposition form (see Appendix)
BIU -	Business Innovation Unit - Philips Healthcare business unit (MR, CT, Ultrasound, etc.)
Customer -	Any (a) individual or (b) individual associated with an entity, which purchases or may purchase a Philips product or service. For purposes of this policy, a Third Party who (only) purchases parts and/or labor is not a Customer.
Encryption -	A process of encoding data in such a way that only authorized parties can read it. For the purposes of this document, Encryption must be adequate to comply with applicable legal requirements and at a minimum meet state-of-practice industry standards such as FIPS 140-2 (U.S.), etc.
FRU -	Field Replaceable Unit
FSE -	Field Service Engineer
HIPAA -	Health Insurance Portability and Accountability Act of 1996 (U.S.A. Legislation)
Media -	see 'Storage Media'
Off-site -	Not located or occurring at the Customer's site
Onsite -	At the Customer's place of business / where the equipment is normally installed

Personal Data - Any information relating to an identified or identifiable individual.
If information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered Personal Data
Note: where this procedure uses Personal Data, this is equivalent to the term Personal Information (or similar) that may be used in other organizations, contracts, laws etc.

PH - Philips Healthcare

PHNA - Philips Health Systems (Global Sales and Service) – North American Market

PH Equipment - Medical device manufactured by or for PH (Philips Healthcare) and sold or leased by Philips Healthcare.

PHI - see Protected Health Information

Philips Healthcare representative / Philips representative – Typically the Field Service Engineer or other designated service representative of Philips. Anyone (employees, distributors, third party contractors etc.) providing services on behalf of or in the name of Philips Healthcare.

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 U.S. HIPAA legislation, Part II, 45 CFR 164.501.

Sanitization - The removal of data from a system or Storage Media with the intent that the data cannot be reconstructed by any known technique. e.g. de-gaussing, overwriting, etc., as appropriate for the specific medium. Sanitization must be adequate to comply with applicable legal requirements and, at a minimum, meet state-of-practice industry standards such as NIST SP 800-88 (U.S.), etc.

Sensitive Data - Personal Data that reveal an individual's racial or ethnic origin, political opinions or membership of political parties or similar movements, religious or philosophical beliefs, membership of a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offences, criminal records, proceedings with regard to criminal or unlawful behavior, or personal identification numbers issued by the government.

Note: in some countries other types of Personal Data may be qualified as Sensitive Data as well (for example 'nationality,' 'age' or 'personality'). In the USA, certain health-related Sensitive Data, generated in certain circumstances, is known as Protected Health Information (PHI).

Storage Media - Any electronic, electromechanical, optical, biological or chemical media or device that has the purpose to persistently store data.

For other abbreviations, refer to the Philips Acronym database on the Philips Intranet.

3.0 CONTENTS

Philips Customer Services employees, distributors and third party service personnel performing service in the name of Philips Healthcare are responsible to complete Authorization of Media Disposition (AoMD) forms as described herein when handling physical Storage Media removed from a Philips Healthcare product at a Customer site. The same Philips representatives are responsible to store completed and signed AoMD forms at the relevant Philips service office.

3.1 Introduction

Storage Media may contain Personal Data and shall be handled in a way that is consistent with the requirements of Philips Healthcare Privacy Policy UX 00035, to avoid the disclosure of Personal Data. Philips Healthcare Customer Services has established the *principle* of not removing unencrypted or un-sanitized Storage Media containing Personal Data from Customer sites whenever feasible - due to the difficulty in complying with the wide variety of changing Customer, local and national government privacy rules and regulations. The conditions for the exceptions to this principle are defined in this policy.

Note: Some Customers have specific contractual restrictions written into purchase or service agreements with Philips that prohibit Philips from removing Storage Media from the Customer's control. If there is a conflict between a contractual agreement and this procedure, the contractual obligation shall prevail.

3.1.1 Standard handling of Storage Media containing Personal Data

The following process outlines the responsibilities of Philips Healthcare representatives that remove Storage Media or come into possession of Storage Media removed from a Philips product as part of a service episode, whether the Storage Media is defective or not, whether the Storage Media itself is a standalone Field Replaceable Unit (FRU) or part of a larger FRU or subsystem. In all cases, unencrypted or un-sanitized Storage Media containing Personal Data shall remain with the Customer unless covered by one of the exceptions in section 3.1.2.

General procedure:

A. Remove the Storage Media from the system.

B. The Philips Healthcare representative (e.g. Field Service Engineer) completes the media identification section of the AoMD form providing a Storage Media description (e.g. serial number, type, etc.) in the Media description field.

C. Check the appropriate check-box(es) on the AoMD form (see Appendices A and B).

D. Have the Customer sign the AoMD form. If a Customer signature cannot be obtained, follow instructions in section 3.1.4, "If no Customer authorization / signature can be obtained."

E. Leave the Storage Media with the Customer.

F. The completed and signed (when applicable) AoMD form shall be retained together with the other service reports/records of the Customer site kept by Philips. A copy of the signed form should be provided to the Customer.

3.1.2 Exceptions to the general Storage Media handling procedure

In all cases, Storage Media can only be removed from Customer sites if the Customer has signed the AoMD form - check box 2 or 3 or the Philips representative has signed the form - check box 'd'.

3.1.2.1 Storage Media containing no Personal Data / Storage Media Sanitization / Storage Media Encryption

If the Philips service representative certifies (by signing the AoMD form, check box 'a' or 'b') and/or if the Customer otherwise agrees and verifies in writing (by signing the AoMD form, check box 2) that the Storage Media contains no unencrypted Personal Data, then the Storage Media may be removed by Philips from the site. (e.g. if the Storage Media is free of unencrypted Personal Data prior to it leaving the site AND Philips specifically desires the return of the Storage Media.

Note: The Customer may elect to perform (non-destructive) Storage Media Sanitization or Encryption themselves, or contract an outside 3rd party or use a Philips product feature (if available) to Sanitize or Encrypt the Storage Media. In some cases, for some products, Personal Data may already be "encrypted-at-rest" or the Philips service representative may have the ability to perform on-site Storage Media Sanitization or Encryption following Philips documented procedures. Philips employees performing Storage Media Sanitization / Encryption can provide the Customer verification by completing the bottom portion of the AoMD form - checking the appropriate box ('a' or 'b') and signing. For the purposes of Philips employees Sanitizing or Encrypting data, only Encryption and Sanitization procedures documented in the Philips product documentation or in service documentation for the specific product / Storage Media in question are acceptable.

3.1.2.2 Storage Media needed by Philips for Off-site analysis / troubleshooting

At times it may be desirable during the provision of service, to remove Storage Media from the Customer's site for further analysis by Philips Healthcare support organizations, such as the Business Unit's tier 3 support organization. This can be the original Storage Media or physical copies thereof. If physical Storage Media are to be removed from the Customer's site in such cases, the Customer must sign the AoMD form (check box 2 or 3) before the Storage Media, together with a copy of the signed AoMD form, is sent to the appropriate Philips support organization.

Note: Different Customer institutions may have unique/different requirements and restrictions for shipping Personal Data. Leaving the responsibility for shipping arrangements to the Customer – whenever possible - helps ensure that each Customer's specific and unique shipping requirements and restrictions are observed. However, in some cases, Philips or the Customer, may prefer that Philips handle the Storage Media shipping - which is also acceptable provided the Customer does not object to Philips to handle the shipping of the Storage Media.

3.1.2.3 Off-site data recovery

At times Philips may be requested by Customers to help recover data from defective hard drives. If data recovery requires removal of Storage Media from the Customer's site and Philips agrees to assist, the Customer must sign the AoMD form (check box 2 or 3) before the Storage Media, together with a copy of the signed AoMD form, is sent to the appropriate Philips support organization or 3rd party location.

Note: Different Customer institutions may have unique/different requirements and restrictions for shipping Personal Data. Leaving the responsibility for shipping arrangements to the Customer – whenever possible - helps ensure that each Customer's specific and unique shipping requirements / restrictions are observed. However, in some cases, Philips or the Customer, may prefer that Philips handle the Storage Media shipping - which is also acceptable provided the Customer agrees and explicitly authorizes Philips to handle the shipping of the Storage Media.

3.1.2.4 Other exceptions

Some Storage Media are unique, rare, or otherwise particularly valuable to Philips (as 'repairable' spare parts) and Philips may desire their return even if the Storage Media contains Personal Data and cannot be Sanitized or Encrypted in the field. In such cases, the Philips representative shall attempt to obtain Customer agreement and a Customer signature (AoMD form - check box 2 or 3) before the Philips service representative removes the Storage Media from the Customer's site. If no Customer signature can be obtained but there are otherwise no contractual restrictions on removing Storage Media, the Philips representative shall sign the AoMD form (check box 'd') and return the Storage Media to the appropriate Philips parts return location.

No other service procedures for handling Storage Media from Customer systems are authorized without the explicit approval of the responsible Philips PHNA Privacy Officer.

3.1.3 Obligations of the respective Philips organization receiving or retaining the Storage Media

When Storage Media is transported to a Philips-controlled facility, it shall be handled in a controlled environment and, at a minimum, access to the Storage Media shall be limited to authorized persons and all Storage Media access shall be logged and any Storage Media Sanitization or destruction shall be performed according to applicable Philips guidelines. See Appendix C.

Any data retrieved from the Storage Media and any copies thereof shall be handled per Philips internal processes.

3.1.4 If no Customer authorization / signature can be obtained

If a Customer signature cannot be obtained for any of the three Customer choices on the AoMD form, the local Philips representative must decide whether to leave the Media at the customer site with the Customer or to arrange for local media sanitization/destruction. Unless there is a belief/concern/suspicion that the Customer desires to retain the media, local sanitization/destruction by Philips is the preferred action.

> If the Storage Media is to be left at the Customer site, the Customer shall be notified of the Storage Media's location and the Philips representative shall describe this location and identify the specific Customer recipient in the AoMD form.
>
> Otherwise, the Philips representative shall make arrangements for local media sanitization/ destruction and describe this final disposition in the AoMD form. See Appendix D.

The local Philips representative shall complete the top part of the AoMD form (noting the drive serial number and Storage Media type in the Storage Media Description field at the top), check the appropriate "Unable to obtain Customer signature…" box 'c' or 'd,' and sign the form in the provided space at the bottom. A copy of the signed AoMD form shall be given to the Customer and the original, together with any sanitization/destruction certifications received - if applicable - shall be retained together with the other related service reports/records of the Customer site kept by Philips. (e.g. the responsible Philips service office).

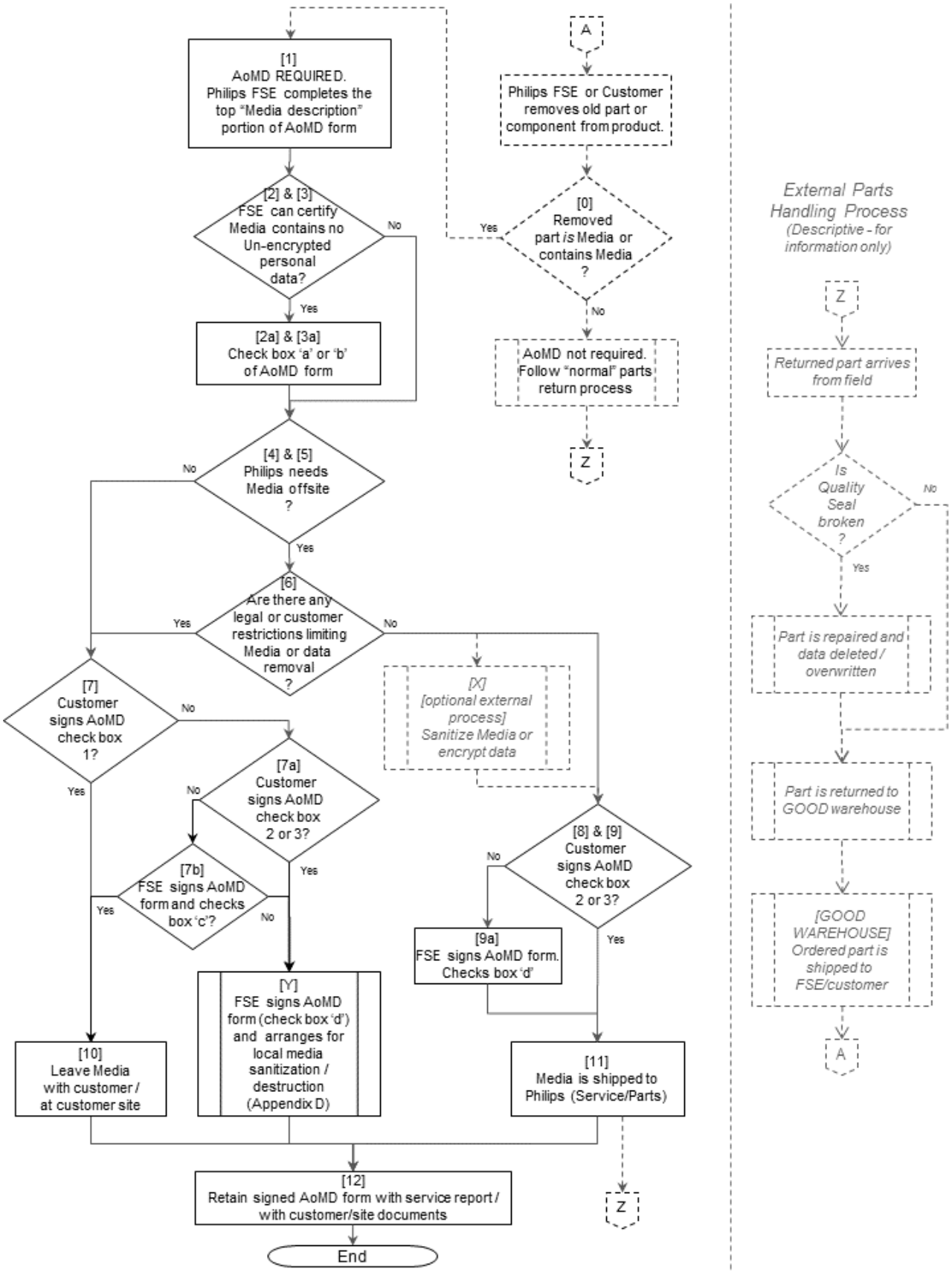
4.0 REFERENCED DOCUMENTS

- UX00035, Philips Health Systems Privacy Policy
- 5104-0143, Protected Health Information (HIPAA) Policy

5.0 APPENDICES

Appendix A: Storage Media Disposition Procedure Flowchart
Appendix B: Authorization of Media Disposition (AoMD) form
Appendix C: Storage Media handling – recommended minimum guidelines
Appendix D: Storage Media handling – local / “field” media destruction

Appendix A: Storage Media Disposition Procedure Flowchart



Appendix A (cont.): Storage Media Disposition Procedure Flowchart – Description of Steps:

[Step 0] If the part is non-volatile Storage Media or might contain non-volatile Storage Media – or if the Philips representative is not 100% certain that the part does not contain non-volatile Storage Media, answer "Yes"

Step 1 Complete the Storage Media identification part of the AoMD (AoMD) form.
Upon removal of Storage Media from a Philips Healthcare product, Philips Healthcare representative fills in his/her name, Customer name / location and the Storage Media-identifying data required in the form. Device serial number(s) must be included if available / identifiable. Proceed to Step 2

Step 2 Does the Storage Media potentially contain Personal Data?
The Philips representative shall not certify this state unless the Storage Media verifiably contains no Personal Data. This can only be verified if the Philips representative Sanitizes the Storage Media (or at a minimum all partitions that could contain Personal Data) via a Philips-approved Sanitization process appropriate for the device in question, or there is Philips-documentary evidence that the Storage Media in question cannot (by design) contain Personal Data. Only if the Philips representative is certain the Storage Media does not contain Personal Data, proceed to Step 2a.
Otherwise, proceed to Step 3.

Step 2a The Philips representative checks box 'a' in the AoMD and signs. Proceed to Step 4.

Step 3 Is the Storage Media Encrypted or is, at a minimum, all Personal Data on the Storage Media Encrypted?
The Philips representative shall not certify this state unless the Storage Media verifiably contains no unencrypted Personal Data. This can only be certified if the Philips representative Encrypts the Storage Media via a Philips-approved Encryption process appropriate for the device in question, or there is Philips-documentary evidence that the Storage Media or, at a minimum, all Personal Data on the Storage Media is Encrypted. Only if the Philips representative is certain all Personal Data on the Storage Media is Encrypted, proceed to Step 3a.
Otherwise, proceed to Step 4.

Step 3a The Philips representative checks box 'b' in the AoMD and signs. Proceed to Step 4.

Step 4 Is the data together with the Storage Media needed by Philips off-site for troubleshooting, etc.? Does Philips service need to transfer this Storage Media off-site in order to fulfill a service obligation to the Customer? If "yes," proceed to Step 6. If "no," proceed to Step 5.

Step 5 Is the Storage Media (just the hardware, the physical *part* but not the data) needed by Philips? If the part is designated by Philips as "Repairable" (i.e. the part is not "Consumable") the answer is 'yes' and proceed to Step 6. Otherwise the answer is 'no' and proceed to Step 7.

Step 6 Can the Philips service representative reasonably confirm that there are no restrictions (local laws / regulations, specific conditions written into the purchase agreement or service agreement, verbal instructions from the Customer, etc.) that would prohibit Philips removal of Storage Media and/or Personal Data from the Customer's site? If yes, proceed to Step 7. Otherwise, proceed to step 'X' (optional) or Step 8.

Step 7 Did the Customer sign the AoMD form, check box 1?
Whenever Customers receive Storage Media from Philips that potentially contain Personal Data, Philips requests Customers acknowledge in writing that they understand that the Storage

Media may contain Personal Data (Encrypted or unencrypted) and that they may have obligations under their institutions' policies for the proper disposal of the Storage Media / data. If the Customer signs, proceed to Step 10. Otherwise, proceed to Step 7a.

Step 7a If a customer signature cannot be obtained for check box 1.
Request that the Customer sign after checking check box 2 or 3 (if/as appropriate). If the Customer does not check any of those three boxes, proceed to Step 7b. Otherwise proceed to Step Y.

Step 7b The Philips representative checks box 'c' or 'd' in the AoMD and signs.
A Customer may be unwilling to sign the AoMD or it may not be feasible to identify and/or obtain a signature from an appropriate Customer representative in a reasonable timeframe. If there are legal or contractual reasons why the media must remain on-site, then the Philips representative checks box 'c' and signs the AoMD form. Otherwise, without a Customer signature, the local Philips representative must decide whether to leave the Media at the customer site or to arrange for local media destruction. Unless there is a reasonable belief/concern/suspicion that the Customer desires to retain the Storage Media, the Media shall be sanitized or destroyed locally by Philips. If the Philips representative believes the customer does not wish Philips to destroy the media, the media shall be left with the customer.

In either case, in the space provided in the AoMD form, the Philips representative shall check the appropriate box ('c' or 'd') and record the required information: The name of the customer representative who received the Storage Media – and its location or; The details of the media sanitization/destruction. Proceed to Step Y if local destruction/sanitization will be performed by Philips or proceed to Step 10 if media is to be left with Customer.

Step X [Optional process step - Encryption or Sanitization via external process – if available]

If the Customer has the ability to Sanitize or Encrypt the Storage Media / Personal Data, the Philips representative should request/allow the Customer to do so. Once completed, proceed to Step 8.

Otherwise, the Philips representative should attempt to Sanitize (unless data is needed for troubleshooting) or Encrypt the Storage Media following a documented Philips Sanitization / Encryption process for the product – but only if such a Philips-documented process exists. In both cases, ensure the Sanitization / Encryption is successful and satisfies any contractual restrictions on Storage Media / Personal Data removal. The Philips representative checks check box 'a' or 'b' of the AoMD form as appropriate and signs the AoMD. Proceed to Step 8.

Step Y Local Storage Media destruction (see Appendix D).

Step 8 Did the customer sign the AoMD form, check box 2?
If "yes," proceed to Step 11. Otherwise, proceed to Step 9.
A customer signature (with check box 2 or 3 of the AoMD form checked) is still desirable even if a Philips representative certifies the Storage Media does not contain Personal Data.

Step 9 Did the customer sign the AoMD form, check box 3?
A customer signature (with check box 3 of the AoMD form checked) is desirable whenever Storage Media containing unencrypted Personal Data is to be removed from the customer's control by Philips Customer Services. If the customer agrees and signs, proceed to Step 11. Otherwise, proceed to Step 9a.

Step 9a The Philips representative checks box 'd' in the AoMD and signs.
Proceed to Step 11.

Step 10 Leave Media with customer / at customer site. A copy of the Philips-signed AoMD form shall be given to the Customer. Proceed to Step 12.

Step 11 Return Media to Philips.
Proceed to Step 12.

Step 12 Retain the completed and signed (when applicable) AoMD form together with other service reports/records of the customer site kept by Philips. A copy of the signed form should be provided to the Customer.

Appendix B: Authorization of Media Disposition (AoMD) form

This section to be completed by a Philips Healthcare representative:

Name of Philips Healthcare representative: _____

Name and location of data owner (Institution): _____

Media description: _____

_____

Describe the media thoroughly including where it came from (what medical system/product), format (HDD, CD-R, DVD, MOD, floppy, DV Tape, etc.), physical description (color, manufacturer, etc.) and especially any unique printed identifiers on labels, (title, serial numbers, dates, etc.). NOTE: Do NOT record here any Personal Data (patient names, patient address(es), birthdates, patient ID #s, etc.)

This section to be completed and signed by an Authorized Representative of Institution. Check only one box:

I, the undersigned Representative of Institution hereby

☐ ***(BOX 1 = MEDIA IS RETAINED BY INSTITUTION)***
acknowledge that the above described Media was received by me on this date from the above Philips Healthcare representative. I have accepted possession of this Media on behalf of Institution for proper disposition in accordance with the policies of Institution. **I understand that the reason I have been asked to take custody of this Media on behalf of Institution is that such Media may contain unencrypted confidential or other proprietary information of Institution, its employees or its patients.**

☐ ***(BOX 2 = MEDIA CONTAINS NO UNENCRYPTED PERSONAL DATA - OK to RETURN TO PHILIPS)***
request Philips Healthcare take possession of the above described Media and its contents. I understand that the Media does not contain any individually identifiable information, including Protected Health Information (PHI), of the Institution or its employees or patients, The Media has either never contained such information or the information has been Encrypted or has been deleted according to the Institution's internal policies. I understand Philips may elect to sanitize (as necessary) and then reuse or sell this Media or otherwise securely dispose of the Media and its contents following Philips procedures and any contractual obligations with Institution.

☐ ***(BOX 3 = MEDIA MAY CONTAIN UNENCRYPTED PERSONAL DATA- OK to RETURN TO PHILIPS)***
request that Philips Healthcare take possession of the above described Media and its contents. I understand that the Media may contain Institution's confidential data, including Protected Health Information (PHI) and that Philips will use reasonable safeguards to prevent unauthorized disclosure of data in accordance with governing law, Philips policies and any contractual obligations with Institution. I understand Philips may elect to sanitize and then re-use or sell this Media or otherwise securely dispose of the Media and its contents following Philips procedures and any contractual obligations with Institution.

_____ _____
Signature of Institution's Representative Date

_____ _____
Print Name of Institution's Representative Telephone # and/or e-mail address of Inst.'s Rep.

_____
Title of Institution's Representative

This optional section to be completed by a Philips Healthcare representative, if necessary. Check as many boxes as apply:

☐ **(BOX a) =** I certify that the Media does not contain Personal Data (i.e. has never contained Personal Data or has been sanitized (data overwritten at least once) in order to erase all Personal Data - including PHI as defined by HIPAA)

☐ **(BOX b) =** I certify that all Personal Data (including PHI) contents of the Media are encrypted

☐ **(BOX c)** = Customer declined to provide signature. I left the Media with Institution at_____ (specific location or recipient name)

☐ **(BOX d)** = Customer declined to provide signature but otherwise did not object to removal of Media from Customer site. I shipped the Media to _____ (Philips location) or destroyed/sanitized it locally by _____

Signature of Philips Healthcare Representative: _____ Date: _____

Print Name of Philips Healthcare Representative: _____

Appendix C: Storage Media handling – recommended minimum guidelines

Philips handling of Digital Storage Media must always be in accordance with applicable Philips, Philips Healthcare and individual Philips business unit policies and procedures. Such policies and procedures must cover – at a minimum - the following.

When Storage Media is physically transported to a Philips-controlled facility, it shall be handled in a secure and controlled manner.

1. Receipt and Shipping of Media into and out of Philips facilities shall be only via reliable / secure couriers. At a minimum, shipping methods must be used such that Philips can reliably track the shipping of - and ensure positive receipt (e.g. via signature) of - any Media containing customer confidential data that is shipped into or out of Philips facilities.
2. Physical and logical access to the Storage Media and its contents shall be restricted to only authorized persons with a legitimate business need for access. Media must be kept in access-controlled areas and/or in access-controlled (e.g. locked) cabinets.
3. Access to Storage Media and media contents shall be logged. The log shall indicate, at a minimum,
    a. Who had access to the media (uniquely identify the user)
    b. The date and time and duration of access
    c. (If possible) What specifically was done to / with the data? i.e., data viewing, data copying, reformatting, etc.

If any Media Sanitization or destruction is performed on customer Media in Philips control, it shall be performed according to applicable Philips guidelines. At a minimum:

4. Media Sanitization – if performed – shall meet applicable and recognized industry-standard sanitization guidelines appropriate for the sensitivity of the data being sanitized (e.g. NIST SP 800-88 Guidelines for Media Sanitization)
5. Media Destruction – if performed – shall be performed consistent with applicable and recognized industry-standard destruction guidelines (e.g. NIST SP 800-88 Guidelines for Media Sanitization) such that data cannot reasonably be retrieved from the destroyed media.

Any duplicate Media created shall be handled in the same way and any copies of data retrieved from the Storage Media shall be handled per applicable Philips internal security and privacy policies and processes.

In all cases, Media content that is no longer needed for legitimate business purposes shall be promptly deleted / rendered inaccessible. Data retention should not exceed 90 days after troubleshooting / data recovery efforts have concluded unless a compelling legal or regulatory requirement for longer retention is identified.

Appendix D: Storage Media handling – local / "field" media destruction

As described in Appendix A, Steps 7, 7a and 7b, if Storage Media removed from a medical device is classified as a "Consumable" part in Philips parts system *but* the Customer will not agree to take possession of the media and/or to take responsibility for the secure disposition of data on the media, the Philips representative should attempt to get the customer to check Box #2 or #3 (as appropriate) of the AoMD form and provide his/her signature and date. If the customer does not sign the AoMD in this case, the FSE / Philips rep should check box "d" of the AoMD and sign the AoMD instead.

As soon as feasible, the Philips representative shall securely "sanitize" or destroy the hard disk drive/media either by using a documented Philips procedure / tool specifically designed for this or by using an appropriate third party media destruction service that can provide certification of destruction. In all cases, any media destruction/sanitization shall be performed consistent with reasonable and appropriate industry standards.

1. Media Sanitization shall meet applicable and recognized industry-standard sanitization guidelines appropriate for the sensitivity of the data being sanitized (e.g. NIST SP 800-88 Guidelines for Media Sanitization)
2. Media Destruction shall be performed consistent with applicable and recognized industry-standard destruction guidelines (e.g. NIST SP 800-88 Guidelines for Media Sanitization) such that data cannot reasonably be retrieved from the destroyed media.

In the AoMD box "d" blank, the Philips representative shall indicate where / how the media was ultimately sanitized / destroyed.

If at all possible / feasible, this media destruction / sanitization shall take place *before* removing the media from the customer's facility. If this is not feasible and there are no contractual restrictions on media removal, the Philips representative shall protect the Media from theft or loss or unauthorized access and - as soon as feasible - sanitize or securely destroy the Media and obtain documented certification of the sanitization/destruction.

Fees for media destruction/sanitization shall be borne by Philips or charged to the customer depending on local contractual agreements or at the Philips Region Service Manager's discretion.

Notes: Illustrative sample of Media destruction services In the USA:

Note: Philips has not necessarily evaluated the following media destruction providers but if no "Philips-recommended" service/vendor is reasonably available, the local Philips representative / Region Service Manager shall exercise reasonable judgment in selecting an appropriate media destruction service.

Some third party destruction services will come on-site to pick up media / drives and provide a certification of destruction once the media destruction completed. Only if/when no such on-site pickup service is reasonably available - at a reasonable cost / in a reasonable timeframe - the Philips representative may hand-carry the media to an appropriate third party destruction location.

Example of media destruction services / pricing (c. 2015-July).

- **Iron Mountain,**
- **Shred-It,**
- **etc.**

Shred-It:

- "Off-site" destruction. If you hand-deliver a single disk drive to a Shred-It location, Shred-It will destroy the media (e.g. disk drive) for $15.00 (+ tax?) and then give you a certificate of destruction.
- "Pickup service" (followed by off-site destruction). Shred It will drive out to your location (the hospital) and pick up the media/drive(s), give you a receipt and take responsibility for its transport and eventual destruction. And they will give you a certificate of destruction once completed for $12.50 per drive (but with a $110 minimum per pickup).
- "Pickup service with immediate *on-site destruction*." For a slightly higher minimum charge ($125) Shred It will drive out to your location and pick up the drive(s) and destroy them immediately (in their truck) before departing. And they will (presumably) give you the certificate of destruction immediately.

******END OF DOCUMENT******