PHILIPS HEALTHCARE

Trainee Name:	
Trainee Signature:	
Date:	

Course Title	Local Course Code	Revision
Protected Health Information (HIPPA) Policy	5104-0143	F

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: **5104-0143 F**

Title: # Protected Health Information (HIPAA) Policy

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
	Director, Business Operations	Robert Seifert	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
F	Minor	Deleted some older URLs in Appendix
E	Minor	Updated "Designated Users," terminology
D	Minor	Update designated users' names; replace "GSSNA" with "PHNA;" add new "Designated Users;" add "...(HIPAA)..." in policy title for clarity in training recordkeeping
C	Major	Updated most text to be consistent with new Philips Privacy policies / codes / guidelines and the updated HIPAA laws (through ARRA / HITECH)
B	Minor	Added Addendum for De-Identification of PHI
A		Initial release.

1.0 PURPOSE AND SCOPE

The Philips General Business Principles require all Philips STAFF to protect the confidential information of Philips, its customers and third parties (including patients). In 1996, the U.S. Federal Government enacted the Health Insurance Portability and Accountability Act (HIPAA), which included various protections for health-related or Protected Health Information (PHI)[1]. Additionally, in 2009, the American Reinvestment and Recovery Act (ARRA) specifically, the HITECH portion, modified HIPAA, and imposed further requirements on both Covered Entities[2] and Business Associates. These HITECH provisions subject Philips to requirements that were once predominantly applicable to Philips customers and a limited portion of Philips businesses. Among other things, the HITECH[3] requirements impose additional breach notification obligations, change aspects of Philips marketing activities, directly require Philips' adherence to HIPAA Privacy and Security Rules, and establish additional controls on how Philips may process SENSITIVE DATA (PHI).

The Philips Privacy Rules for Customer, Supplier, Business Partner Data (CSB) provide a framework of requirements for PERSONAL DATA PROCESSING. The Philips Health Systems Privacy Policy further defines compliance for responsible STAFF PROCESSING of PERSONAL DATA on behalf of Philips. This document provides guidelines for the PROCESSING of PERSONAL DATA, per Article 2.1(i) Philips Privacy Rules (CSB), specifically addressing PROCESSING of PERSONAL DATA where such PROCESSING activities are subject to the US HIPAA and HITECH regulations.

The basic policy hierarchy is:

Philips General Business Principles
- Philips Privacy Code
  - Philips Privacy Rules for Customer, Supplier, Business Partner Data (CSB)
    - Philips [Health Systems] Privacy Policy
      - Philips organization policies, procedures & guidelines (including this policy)

The intended audience of this document is any Philips STAFF who PROCESSES PERSONAL DATA per Article 2.1 or 4.1, CSB Privacy Rules, where the PROCESSING ACTIVITY is subject to US HIPAA regulations.

In any cases where there is a potential conflict between these guidelines and its precedents, the Philips RESPONSIBLE EXECUTIVE (RE) should consult with the appropriate Privacy Officer and/or the Philips Chief Privacy Officer. (Article 1.9 CSB)

[1] For the purposes of this guidance, Protected Health Information (PHI) is a complete subset of SENSITIVE DATA which is a subset of PERSONAL DATA as those terms are used in Philips Policies, Codes and Guidelines. Though Philips Customers may refer to PERSONAL and SENSITIVE DATA as "PHI," "e-PHI," "Individually Identifiable Health Information or IIHI," these terms all fall under the Philips Privacy Rules' definition of PERSONAL DATA, and are collectively referenced in this document as PERSONAL DATA.

[2] Covered entities, generally, are healthcare providers, clearinghouses, etc. (Philips Customers, hospitals, physicians, etc.). Some of Philips businesses are covered entities, though generally, Philips Health Systems operates as a "Business Associate" of Philips customers (in the sale and service of PH products and services).

[3] The "HITECH" portions of the U.S. American Recovery and Reinvestment Act of 2009 (ARRA) legislation clarifies and in some cases redefine some of the obligations of Business Associates under HIPAA.

2.0 EXPLANATION OF KEY TERMS

ARRA	U.S. American Recovery and Reinvestment Act of 2009.
Business Associate	Firms or persons performing certain services for or on behalf of COVERED ENTITIES as defined in HIPAA and ARRA.
Covered Entity	Health Plans, Health Care Providers, and Health Care Data Clearinghouses as defined in HIPAA and ARRA.
CSB	Customer, Supplier, Business Partners
HIPAA	Health Insurance Portability and Accountability Act of 1996 (U.S.)
HITECH	Together, title XIII of Division A and Title IV of Division B of ARRA are known as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act." Section 13401 (re: HIPAA Sect. 164.308 admin controls, .310 physical, .312 technical, .316 documentation) defines the application of HIPAA to Business Associates.
PH	Philips Health Systems, Philips Healthcare (deprecated) or Philips HealthTech
PHNA	Philips Health Systems, Philips Healthcare (deprecated), Philips HealthTech (Sales and Service) North America
Personal Data	PERSONAL DATA shall mean any information relating to an identified or identifiable individual where the individual is associated with a Philips Customer, Supplier or Business Partner.
Privacy Event	PRIVACY EVENT is defined as a set of circumstances where there is evidence that a person or IT-based application has engaged in unauthorized processing of PERSONAL DATA.
Processing	PROCESSING shall mean any operation that is performed on PERSONAL DATA, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of PERSONAL DATA.

Protected Health Information (PHI) PERSONAL DATA that relates to an individual's health condition, diagnosis or treatment or payment for her health care, and from which the individual's identity may reasonably be determined. An example of Protected Health Information is a medical image or report that contains or refers to a patient's name, medical record number, social security number, address, etc.

PHI does not include health information from which all information that could be used to identify the individual, e.g., name, address, date of birth, medical record or other identifying number, has been removed (adequately "de-identified").

NOTE: De-identification may only take place under the guidance of the appropriate Privacy Officer.

Responsible Executive (RE) Defined as the lowest-grade Philips business executive who has primary budgetary ownership over the relevant PROCESSING.

Security Event SECURITY EVENT is defined as an observable occurrence leading to either or both of the following:

- Philips software or data that is managed by a Philips product is suspected of being maliciously altered, misused or lost (includes virus, worm, hackers, etc.)
- A Philips system or component has a customer-reported security vulnerability that could result in alteration, misuse or loss

Sensitive Data SENSITIVE DATA shall mean PERSONAL DATA that reveal an individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.

Staff STAFF shall mean all Employees and other persons who process PERSONAL DATA as part of their respective duties or responsibilities using Philips information technology systems or working primarily from Philips premises.

3.0 INSTRUCTIONS FOR HANDLING PROTECTED HEALTH INFORMATION AND OTHER PERSONAL DATA

3.1 Exposure to Personal Data

Philips STAFF may be exposed to PERSONAL DATA (including PHI) during Philips customer site visits, demonstrations, product problem definition, service and support activities, including product or part returns, and many other customer-facing activities. The following guidelines apply to Philips STAFF PROCESSING PERSONAL DATA, whether PROCESSING involves transfer of PERSONAL DATA or PROCESSING within Philips or externally (to non-Philips parties). The Philips Privacy Rules provide a framework for appropriate PROCESSING and for the protection of PERSONAL and SENSITIVE DATA privacy. This **Protected Health Information Policy**, however, specifically addresses requirements under the HIPAA Privacy and Security Regulations, as modified by HITECH.

3.1.1 *Seek guidance* from the appropriate Philips Privacy Officer as questions arise regarding PERSONAL DATA PROCESSING or this process.

3.1.2 *Contact* the Philips North America Credentialing Office if approached by a customer about HIPAA training.

3.1.3 *Minimize exposure* to PERSONAL DATA to only that data which is absolutely necessary.

3.1.4 *Take appropriate steps* to secure PERSONAL DATA to prevent unauthorized use or PROCESSING.

3.1.5 *Ensure* that any system (e.g., PC, laptop, etc.) used for the processing of PERSONAL DATA is encrypted as required by Philips IT Security policies: *Laptop Management Policy* (see Addenda 5.1 for URLs)

3.1.6 *Ensure* any PERSONAL DATA located, stored, or transported on removable media is encrypted per Philips encryption guidelines, e.g. *Field to Factory Encryption Guidelines* (see Addenda 5.1 for URLs).

3.1.7 *Follow* Philips customers' local policies regarding PERSONAL DATA.

3.1.8 *Immediately report* any PRIVACY or SECURITY EVENT to the appropriate Philips Product Security or Privacy Officer. For security events in service, follow 5104-0025 Philips *PHNA Customer Escalation Management Process* and/or 5100-0040 *Customer Feedback Procedure* as appropriate. In addition, for all privacy events, use the *Philips Privacy Event Reporting Form* on the Privacy Event Reporting Site (see Addenda 5.1 for URLs).

3.1.9 *Do not solicit* information about <u>any patient</u>, <u>at any time</u> during the performance of official Philips business unless doing so is necessary for the Philips personnel to perform a service obligation to the customer. This includes speaking to hospital personnel about any past, current or future patient's condition or status, while on the customer's site, or in communication with any customer employee or representative.

3.1.10 *Do not remove* or cause to be removed any PERSONAL DATA from Philips Customer premises unless removal is absolutely necessary to the performance of a business purpose allowed under the Philips Privacy Rules ***<u>and</u>*** is explicitly authorized by the customer.

3.1.11 *Do not use* or allow to be used any PERSONAL DATA obtained from a Philips Customer for non-service related activities (i.e., training, marketing, communications, sales, etc.) without ensuring appropriate authorization for use of customer supplied data is obtained from the customer, and under guidance of your applicable Philips Privacy Officer.

3.1.12 *Do not use,* disclose, store, capture, or otherwise PROCESS PERSONAL DATA unless specifically permitted under the Philips Privacy Rules[4].

3.2 Business Associate Agreements

United States customers occasionally request that Philips employees sign a (HIPAA) Business Associate Contract or Agreement, which governs the use and disclosure of PHI by Philips. These requests may have the effect of modifying the Philips Terms and Conditions of Sales and Service and should therefore be forwarded, unsigned, to:

- The Account Manager (For sales-related agreements,); or
- The Customer Support Contract representative identified on the Product Security website (for service, support and other agreements)

The relevant Philips credentialing manager can also provide guidance in how to respond to customer requests for verification of a Philips employee's "HIPAA training."

[4] Articles 2.1 and 4.1 of the Philips Privacy Rules for Customer, Supplier, Business Partner Data explicitly state legitimate business purposes for PROCESSING of PERSONAL and SENSITIVE DATA. Where questions exist as to whether a PROCESSING activity meets an Article 2.1 or 4.1 legitimate business purpose, consult with your appropriate Privacy Lead.

4.0 REFERENCED DOCUMENTS [5]

- 5104-0025 Philips PHNA Customer Escalation Management Process
- 5100-0040 Customer Feedback Procedure
- Philips General Business Principles
- Philips Privacy Code
- Philips Privacy Rules
  - ◊ Philips Privacy Rules for Customer, Supplier, Business Partner Data (CSB)
  - ◊ Philips Privacy Rules for Employee Data
- Laptop Management Policy
- Field to Factory Encryption Guidelines
- Privacy Event Reporting Form

[5] links (URLs) for un-numbered documents can be found in the Addenda

5.0 ADDENDA

5.1 External / public URLs:

- Philips Product Security: http://www.usa.philips.com/healthcare/about/customer-support/product-security

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

Protected Health Information (HIPAA) Policy 5104-0143

Bill Stewart
Philips, N. Am. Customer Service, Health Systems
July 13, 2017

innovation + you

PHILIPS

Introduction

The training course you are now viewing must be reviewed by all customer-facing Philips Health Systems employees on an annual basis in order to stay current in relevant Philips privacy policies and regulations. In a relatively short format it summarizes the content and requirements of the Philips privacy guidelines (including recent updates) most relevant to Philips employees.

Reviewing this material should take less than 30 minutes.

Purpose

Governments have enacted laws relevant to privacy and protection of personal information – especially health information. Among other things, these laws establish controls that define how Philips may process sensitive / personal data, including Protected Health Information (PHI), and make clear Philips obligations with regards to privacy breach notifications.

USA: HIPAA, ARRA (HITECH), etc.
Canada: The Privacy Act, PHIPA, PIPEDA, etc.

Philips, and individual Philips businesses have developed relevant Privacy Policies, Codes and Guidelines to address the legal and business obligations in this area.

For Philips employees working in the USA - - - as long as you are complying with Philips Policies, Codes and Guidelines regarding the handling of personal and sensitive data, you meet your obligations under HIPAA for the handling of Protected Health Information (PHI).

Privacy Policy Hierarchy & Overview

Philips General Business Principles require all Philips employees to protect the confidential information of Philips, its customers and third parties (including patients). Philips Privacy Code and Privacy Rules together with Philips (Health Systems) Privacy Policy, procedures and guidelines further specify how Philips employees are to handle personal health data in order to stay compliant with contractual obligations and local and national laws.

Philips (Corporate) General Business Principles:

- Philips Privacy Code:
  - Philips Privacy Rules:
    - Philips Health Systems Privacy Policy (UX 00035):
      - Philips Health Systems organization policies, procedures & guidelines (e.g. 5104-0143 Protected Health Information Policy, others)

Definitions

Personal data - Any information relating to an identified or identifiable* individual where the individual is associated with a Philips Customer, Supplier or Business Partner.

- **Sensitive data -** Personal data that reveals an individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.

  - **Protected Health Information (PHI) –** Defined in U.S. HIPAA legislation - PHI is any personal data that relates to an individual's health condition, diagnosis or treatment or payment for health care, and from which the individual's identity* may reasonably be determined.

*Note: identifying characteristics include not just names and birth dates, but also addresses, phone numbers and several other categories of data. When in doubt, consult with your Philips Privacy Lead / Privacy Officer.

Philips Privacy Compliance Information & Resources for Employees

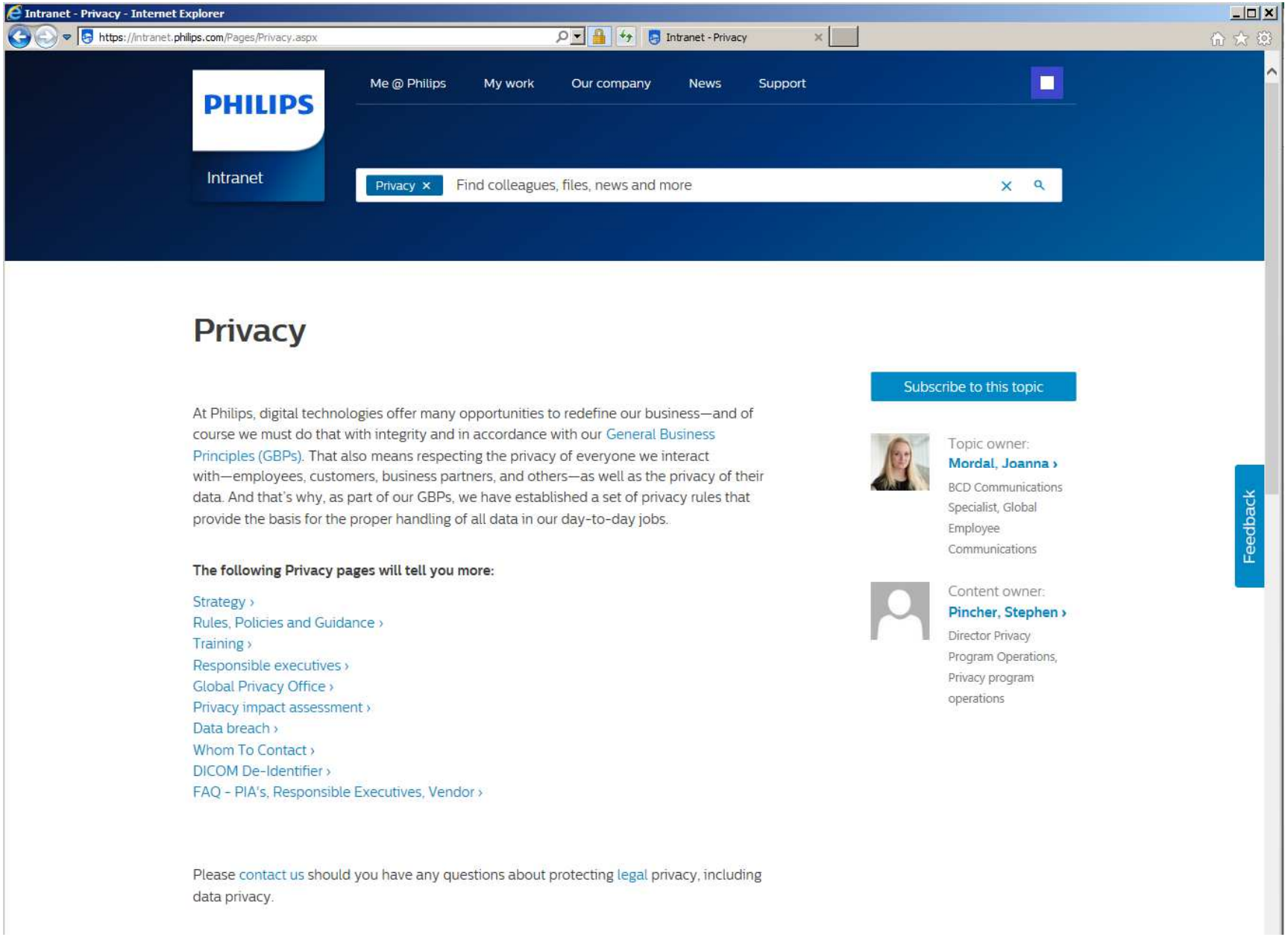
Philips Privacy Resources

Privacy Compliance Intranet Site [https://intranet.philips.com/Pages/Privacy.aspx]

Provides Information on things like:

- Privacy Frequently Asked Questions (FAQ)
- "Whom to contact" (Philips Privacy Officers / Privacy Leads / "Responsible Executives")
- Data Breach / Privacy event reporting,
- Privacy training, resources, announcements and activities, etc.
- Links to Philips General Business Principles, Philips Privacy Code, Philips Privacy Rules, etc.
- Privacy Impact Assessments (PIA)
- etc.

Philips Health Systems Privacy Compliance Intranet



Personal Data Handling

(Including PHI / ePHI = *electronic* Protected Health Information)

Personal Data Handling – Dos and Don'ts

- Seek guidance from Philips Privacy Officer / Privacy Lead whenever questions arise.
- Contact Philips employee "Credentialing" office if customers ask about your HIPAA or "Privacy" training. See: *Philips intranet - Credentialing site* [1]
- Minimize exposure to personal data to only that data which is necessary for your job.[2]
- Take appropriate steps to physically secure personal data in order to prevent unauthorized use or processing.
- Use data/disk encryption on Philips PCs/laptops as required by Philips IT Security policies.
- Encrypt any personal data located, stored, or transported on removable media.
- Follow Philips customers' local policies regarding personal data handling.
- Immediately report any privacy or security event to the appropriate Philips Product Security or Privacy Officer. See: *Privacy Event / Breach Reporting* [1]

[1] https://intranet.philips.com/Pages/U-S-Credentialing.aspx

[2] Articles 2.1 and 4.1 of the Philips Privacy Rules for Customer, Supplier, Business Partner Data explicitly state legitimate business purposes for processing of personal and sensitive data. Where questions exist as to whether a processing activity meets an Article 2.1 or 4.1 legitimate business purpose, consult with your appropriate Privacy Lead.

Personal Data Handling – Dos and Don'ts

- **Do not** solicit information about any patient, at any time during the performance of official Philips business unless doing so is necessary to perform a service obligation to the customer.
- **Do not** remove or cause to be removed any personal data from Philips Customer premises unless absolutely necessary to the performance of a business purpose allowed under the Philips Privacy Rules[2] **and** the removal is authorized by the customer.
- **Do not** use or allow to be used any personal data obtained from a Philips Customer for non-service related activities (i.e., training, marketing, communications, sales, etc.) without ensuring appropriate authorization for use of customer-supplied data is obtained from the customer (under guidance of your applicable Philips Privacy Officer).
- **Do not** use, disclose, store, capture, or otherwise process personal data unless specifically permitted under the Philips Privacy Rules.[2]

[2] Articles 2.1 and 4.1 of the Philips Privacy Rules for Customer, Supplier, Business Partner Data explicitly state legitimate business purposes for processing of personal and sensitive data. Where questions exist as to whether a processing activity meets an Article 2.1 or 4.1 legitimate business purpose, consult with your appropriate Privacy Lead.

Example of contractual obligations:

(excerpt from Philips (HIPAA) Business Associate Addendum (BAA) – often added to service contracts in USA)

"...3.1 Philips agrees to:

- ...Not use or disclose PHI other than as permitted or required...
- ...Use appropriate safeguards...to prevent use or disclosure of PHI...
- ...Report...any use or disclosure of PHI not provided for by this Addendum...
- ...Make its internal practices, books, and records available to the US Secretary of Health and Human Services...
- ...

...3.2 Permitted Uses and Disclosures...

- ...Use or disclose PHI as Philips deems necessary to perform its obligations under the Underlying Contracts or as otherwise permitted or required by law...."

What does this mean for me?
What do I need to look out for?

- Sensitive customer data including Protected Health Information **(PHI) can be acquired unintentionally** – in product log files on FSE laptops; in system 'backup' data on removable media (USB "Flash" memory); etc.
- De-identification can only be properly completed / verified by specifically authorized **people trained in de-identification.** ***This is not you.*** This is not the customer either. Philips shall not rely on customer verbal assurances that clinical data is anonymized or de-identified. When in doubt, consult your Philips privacy lead.
- Philips **laptops and removable media are occasionally lost or stolen** – most frequently from employee cars. All Philips laptop hard drives must be encrypted using the relevant Philips IT-approved encryption method. Personal data on removable media shall also be encrypted when media leaves customer control.
- **Be aware of local customer regulations**. Do not remove personal data / media from customer premises unless it is necessary to do your job *and* you have the customer's permission.

Disposal of Personal Data

Most Philips customers have policies and procedures for disposal of confidential materials, including those containing personal and other sensitive data. If personal data is in your possession - and it is no longer needed for your job – return it to the customer if media is still at the customer site. Otherwise:

- **Paper / film documents & non-re-writable media*** (CD-R, etc.)

  Securely destroy. Do not re-cycle.

- **Re-writable media** (CD-RW, USB/'Flash' memory, etc.)

  Re-writable media must be securely destroyed* or properly "sanitized" before re-use.

- **Re-sale / 'demo' systems (Ultrasound, etc.)**

  Hard drives must be sanitized or replaced before system re-sale / re-use. Refer to the specific modality sales / applications guidelines for the specific product.

* when locally accessible, place into Philips facilities' "confidential materials" / "confidential materials - media" bin for disposal/destruction.

Privacy Event Escalations

Privacy Event Definition

Privacy Event:

The unauthorized disclosure or processing of personal data.

A set of circumstances where there is evidence that a person or IT-based application has engaged in unauthorized processing of personal data.

Privacy Event Reporting

General:

Refer to the on-line Privacy Breach Reporting instructions on the Philips Privacy Compliance Intranet site:

For Field Service employees:

1. Follow Philips Privacy Breach / Privacy Event Reporting instructions (as above) *AND*
2. File a "security-flagged" service escalation

   The Philips "Escalation Management Process" describes how to escalate customer security issues. By definition, privacy "events" or data "breaches" are categorized as *security issues* for the purposes of escalation. OneEMS or Philips Customer Feedback Management (CFM) system - or equivalent replacement - are the appropriate mechanism(s) for Philips Customer Service reporting and escalation of customer privacy-related concerns and events.

Philips Privacy-related Training Courses

Remain up-to-date on all required training in TEDS/TMS and Philips University

Favorites | Philips Training Management System

PHILIPS

Learning Title	Code	Type	Hours
AGILENT PRIVACY PRACTICES	42SN-MKT-WEBPRIV		0.50
Ethics & Privacy Roundtable	Ex-Dunlee547		0.50
Information Protection and Privacy	if1aPHP		1.00
PH Security & Privacy Requirements for Products and Services	UXW-030020 v2		1.00
PHI (PRIVACY HEALTH INFO)	XCTW-0341117/CTBST		1.00
PRIVACY - 2007	pr2aSTD		0.35
Privacy and Data Protection Awareness	LE01.02		1.00
Privacy of Individually Identifiable Health Information	XCTW-0341117 - Review		1.00
Rev A: Privacy of Individually Identifiable Health Information	XCTW-0341117		1.00
Security and Privacy Focus 2007	Sec/Priv 2007		0.50
Security and Privacy Requirements for Products	9020-0362B		0.50
TEDS-DATA PRIVACY AGREEMENT	TEDS-DATA PRIVACY		0.50
VA Information Security Awareness and VHA Privacy Policy Training	VA INFO SEC		1.00

Check TEDS / TMS (Training Management System) to see if you are required to take any of these – or other – privacy courses

Review / Case Studies

Case Study #1

One of the most common privacy violations reported in hospitals is related to hospital staff or vendors, who are not directly involved with the care of a given patient, seeking information about that patient's condition (typically a friend, acquaintance or relative).

Philips personnel may NOT solicit information about <u>any patient</u>, <u>at any time</u> unless doing so is NECESSARY in order for the Philips personnel to perform a service obligation to the customer. This includes speaking to hospital personnel about any past, current or future patient's condition or status, while on the customer's site, or in communication with any customer employee or representative.

Case Study #2

In preparation for a system upgrade, an FSE made a backup of the customer's system – the system (and therefore the backup) included a large database of patient names and patient health data. The FSE left the backup disk in his car for a week while the upgrade was ongoing. That week, the (unencrypted) backup disk was stolen from his parked car. The incident was reported to the customer who did not believe Philips had used "appropriate safeguards" to protect the patients' personal data in this case. The customer made it clear that they would identify Philips as the cause of the personal data loss in any notifications they are required to send to the affected patients.

1. Personal data should not be removed from customer sites unless;
   a) it is necessary to do your job *AND*
   b) It is encrypted (whenever possible/feasible) *AND*
   c) the customer has given you explicit permission for data removal.

2. An unattended car is not a secure location (locked or unlocked, at home or in customer's parking lot)

Case Study #3

An FSE left his service laptop *AND* his laptop backup drive in his car in his driveway when he left for a long weekend vacation. The laptop and backup drive were subsequently stolen while he was away. Although the laptop was encrypted and it is likely no patient data was on the drive / laptop at the time of the theft, Philips was unable to determine for certain what was on the stolen laptop because the backup disk was stolen at the same time.

1. Backup disks should never be stored together with the PC / laptop they back up!

2. An unattended car is *not* a secure location.

Case Study #4

A section of a log file from a defective medical device was copy-and-pasted into an internal Philips service technical escalation file. The log file (incidentally) also contained several patient names. The patient names were not relevant / not needed for the troubleshooting activity.

Do not copy or propagate sensitive customer data when not necessary. In this case, it would have been relatively easy for the FSE to have deleted the patient names from the log file text when copying and pasting the log file excerpt into the internal Philips escalation document. Even when such info is helpful to the investigation, it is advisable to substitute "dummy" patient names for the real names whenever reasonably feasible. e.g. "Patient#1" instead of "John S. Smith."


PHILIPS