

Home Telehealth Capability Enhancements (HTCE)

Integrated Home Telehealth Application (IHTA)

IHTA Access Policy for Patient Sensitive Information



April 2011
Version 1.2

Revision History

The revision history cycle begins once changes or enhancements are requested to an approved IHTA Access Policy.

Date	Revision	Description	Author
06/16/2010	0.1	First draft for review	David Komraus
06/18/10	1.0	Approved	Marcia Dunn
08/12/10	1.1	Updated IHTA User list to match CRUD	David Komraus
04/15/11	1.2	Changed project name to Home Telehealth Capability Enhancements (HTCE)	Katie Shepherd



Table of Contents

1.	Purpose.....	1
2.	Access to Patient Sensitive Information.....	1
3.	Data Access	1
3.1.	Secondary Access.....	2
4.	References	2



1. Purpose

The purpose of this document is to describe the business rules that determine which Integrated Home Telehealth Application (IHTA) users are granted access to Patient Sensitive Information (PSI). For IHTA purposes, PSI is the combination of a patient's name and Social Security Number (SSN). These rules are implemented to ensure that proper levels of security and confidentiality are maintained, while at the same time allowing each user the functionality and information needed to perform his/her job, but nothing more.

2. Access to Patient Sensitive Information

Currently, PSI is only used in the Inventory Tracker module of IHTA. Table 2 shows where PSI is used and displayed in the module.

Table 1: Use of PSI in Inventory Tracker

Function	Inputs	Outputs
Search Device by Patient	Patient First Name Patient Last Name Patient SSN	Patient First Name Patient Last Name Patient SSN

3. Data Access

In addition to being limited by function, access to PSI is also controlled according to organizational boundaries. A user may only access data within his/her own organization and at the lowest organizational level that he/she was approved for during registration approval process. Table 2 outlines this user-limited access in Inventory Tracker.

Table 2: Inventory Tracker's User-Limited Access

IHTA User	Function	Data Range
National Administrator	Search Device by Patient	No patients
Application Administrator	Search Device by Patient	No patients
Management	Search Device by Patient	No patients
VISN Administrator	Search Device by Patient	Own VISN patients
Facility Administrator	Search Device by Patient	Own facility patients
Care Coordinator	Search Device by Patient	Own facility patients
Program Support Assistant	Search Device by Patient	Own facility patients



3.1. Secondary Access

Secondary access policies will be required by the Continuation of Operations Policy (COOP). COOP ensures that the Department of Veterans Affairs (VA) can continue to provide critical services in the event of a system failure or natural disaster that disrupts service delivery in a geographic area. Granting additional access to support the COOP will modify the data ranges presented in Table 2. In a COOP scenario, for example, the Veterans Integrated Service Network (VISN) 1 Administrator may be granted access to VISN 2 patient data, so that the VISN 1 Administrator can assume the duties of the VISN 2 Administrator. In this case, the VISN 1 Administrator would have access to VISN 2 PSI.

The full implications of COOP for PSI access will be added to this document as details become available.

4. References

The following references were utilized to develop this access policy:

1. Privacy Act of 1974, (PL 93-575)
2. VA Directive 6210, Automated Information Systems Security
3. VA Handbook 6500, MP-1, Part II, Chapter 21, Access to VA Systems of Records under the Privacy Act of 1974
4. VA Directive 6500, Information Security Program, dated August 4, 2006
5. VA Handbook 1605.1, Privacy and Release of Information
6. Freedom of Information Act
7. HIPAA 164.308a4iiB, 164.312d.b.
8. Computer Security - A Handbook for VA Managers and End Users