



University of Connecticut Health Center

POLICY NUMBER 2003-32

April 14, 2003

**POLICY: PORTABLE COMPUTING DEVICE (PCD) SECURITY POLICY
(Privacy & Security of Protected Health Information (PHI))**

PURPOSE:

With the growing need for instant communication and data access, a significant increase in the use of Personal Computing Devices has been seen at the University of CT Health Center. This policy is intended to provide guidelines to departments, including residency programs that are utilizing PCD's or considering their implementation in the future. Devices included in this category are: notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs using Windows CE, text pagers and smart phones. Use of PCDs at the Health Center by employees, students and affiliated individuals are governed by this policy. In addition, this policy addresses the use of PCDs in each of the following device ownership scenarios:

- a) Originally purchased by and ownership retained by the Health Center
- b) Originally purchased by the Health Center with ownership transferred to individual employee, student or affiliated individual accepting the device.
- c) Originally purchased and ownership retained by the individual employee, student or affiliated individual.

POLICY STATEMENT:

1. HIPAA Compliance and PCDs

There are a growing number of applications, both commercial and institutionally developed, that allow clinicians to store, view and interact with patient data on their PCD. Federal HIPAA guidelines require institutions to develop policies and protections to secure electronic Protected Health Information (PHI) stored on or accessed from any computing device, including PCDs. This policy addresses this requirement when PCDs are used to access and or store PHI at the Health Center. In most cases, the Health Center's major clinical systems containing PHI are commercial products and as such, the mechanisms enabling PCD connectivity and the associated data protections for HIPAA compliance will be provided by the application vendors' and remain application specific. As a result, PCDs used by clinicians may end up with multiple types of synchronization/real time access software and encryption techniques.

Regardless of whether one or more mechanisms are involved, if the end result is PHI is stored on, viewed by or transacted with from a PCD; the data protections outlined in this policy must be installed and operational on the device.

2. PCD Data Protections – Scope

As the usage of PCDs increases, it becomes more important to protect sensitive data on these systems. Sensitive data includes Health Center locally stored information from email and other datasets classified as registered confidential according to UCHC’s data classification security policy (See attached Data Classification Policy).

Data protections for PCDs used at the Health Center must:

- a) Protect classified Health Center/Patient data stored on the PCD
- b) Protect classified Health Center/Patient data during a synchronization or real time transaction (applies to wire-based & wireless connections)

3. PCD Data Protections – Governing Principles

Given their small size and portable nature, it is more likely that these devices will fall into the wrong hands than a desktop system. However, the same basic principles governing the protection of data on regular desktop systems apply equally to PCDs. These principles are:

- a) If classified data (e.g. PHI) is to be stored locally, it must be stored in an encrypted format. Regardless of the device’s ownership scenario, PCDs are precluded from locally storing this type of data (whether downloaded or manually entered) without first acquiring and installing the local encryption/password protection software.
- b) For PCDs storing registered confidential data as defined by the UCHC Data Classification policy access to all main system functions and data must be protected by a strong password system that meets *UCHC* security requirements (See attached Data Classification Policy). In addition, in this scenario, the required PCD security software must be configured to automatically “lock out” access to the device without first re-entering the authorized user ID and password.
- c) If classified data is transferred/synchronized either via wire (UCHC LAN/WAN or Public Internet) or wireless connections (including to and from web sites, server databases or e-mail servers), it must be transmitted in an encrypted format using the Health Center’s centralized, secure server. Using alternative methods of synchronization including PC/MAC based synchronization software included with the PCD to synchronize with UCHC classified data sources is prohibited and subject to progressive discipline up to and including termination.
- d) Real time access to classified data using internal or public wireless networks requires the installation of the Health Center’s Virtual Private Network (VPN Software) on the PCD. This software will provide for the requisite strong authentication and continuous encryption of the data required by HIPAA.
- e) The process for obtaining the software necessary to secure the Health Center’s classified data when stored, viewed or interacted with via PCD is outlined in attachment 1. The individual or department who own the device must pay for the costs for this software.

- f) Use of the included synchronization software from the PCD manufacturer is permitted when the data sources are not considered classified under Health Center policy.

4. Security Controls – Storage and Synchronization Software Standards

Any PCD is not considered to be a secure computing device unless the UCHC specified, additional security software has been installed. Without this software installed, only non-classified Health Center information may be stored on the device. The required security software must be obtained from and installed by the IT Security Department. In cases where departments or residency programs purchase PCD's in bulk, IT may install all the HIPAA security software prior to the devices being distributed to the intended users.

See attachment 1 for acquisition and support details.

5. PCD Ownership and HIPAA PHI Protection Liability

Table one on page 5 of this policy lists the role types at UCHC most likely to use a PCD involving exposure to Protected Health Information (PHI). The table uses information about ownership of the PCD hardware and software and whether PHI is made available from UCHC clinical systems or is hand entered into the PCD to assign liability for HIPAA compliance. In any scenario where UCHC makes data from clinical information systems available via automated processes or live connections to a PCD, liability remains with the Health Center. See table 1 for details. In cases where the use of a PCD in clinical settings is confined to accessing medical databases, references or calculators and does not involve patient identifiable PHI, HIPAA regulations do not apply and no liability exists.

The institution where a resident is assigned may install software allowing a particular resident to store, view and interact with patient data on their PDA. In these cases, the host institution is assumes any HIPAA liability and is responsible for providing support for the PDA software and hardware installed for this purpose.

6.0 Acquisition:

The Health Center suggests that individual users, departments or residency programs considering acquiring PCDs, carefully examine their requirements. In certain instances, these can be as simple as obtaining Microsoft Outlook email and calendaring data synchronization. Other needs could include specialized accessories including wireless hardware and network services. Thought should be given to whether sensitive UCHC data will be stored on the device.

UCHC Departments considering bulk purchases of PCD's should contact Bob Brandner, George Spangenberg or Brenda Whitehead from IT. IT will work with the ordering department and Purchasing to negotiate optimal equipment and support pricing.

Karen Goodman at the Capital Area Health Consortium (CAHC) is the contact for residency programs contemplating similar volume acquisitions of PCDs. CAHC will assist the residency program directors with negotiating and executing these purchases and any associated technical support arrangements.

7. Asset Management:
PCDs considered to be the property of UCHC will have valid property tags issued by the Materials Management department.

Sandra Armstrong (signed)

2/4/03

Chief Information Officer

Date

Peter Deckers, M.D. (signed)

2/15/03

Executive Vice President for Health Affairs

Date

Replaces: NEW POLICY

Addendum:

Table One

Attachment 1 - Personal Computing Device (PCD) – Acquisition & Support Services

Table One

PCD User Type	Asset Owner	Probable Uses for Device at UCHC or Other Host Institution for UCHC Residents	Owner of Apps on PCD accessing or storing PHI	PHI Automatically Synched from/to UCHC Clinical Apps	PHI User Entered into Stand Alone PCD Medical Apps (e.g. patient tracker)	Liabile Party for HIPAA Compliance for PHI Of UCHC Patients	Required Data Protections For PCD
Clinical Employee	UCHC	-Access to and Interaction with UCHC Clinical Applications and or - Enter patient notes with PHI into local PCD software	UCHC	Yes	No	UCHC	If UCHC owned and PHI feed is automated or PHI manually entered, then UCHC provides: - Strong Authentication - Encrypted PCD Storage - Encrypted transmissions - Device lockout inactivity timer
Affiliated Physician	Individual Physician	- Automated Script printing and or - Enter patient notes with PHI into local PCD software	Individual Physician	No	Yes	Individual Physician if PHI manually entered UCHC if PHI feed is automated	If Individual Physician owned, but UCHC feeds PHI automatically: the UCHC provides - Strong Authentication - Encrypted PCD Storage - Encrypted transmissions

							- Device lockout inactivity timer or If individual physician owned and PHI manually entered, then physician should provide same protections as above.
Resident	Individual Resident	- Access to and Interaction with UCHC Clinical Applications - Automated Script printing - Enter patient notes into local PCD software	UCHC & Individual Resident	Yes	Yes	UCHC if serving as host for Residents and automatically feeding PHI to device. Other Resident host institutions if automatically feeding PHI to device. Individual Resident if PHI is manually entered into Device.	The liable party must provide the following whenever device involves PHI: - Strong Authentication - Encrypted PCD Storage - Encrypted transmissions - Device lockout inactivity timer
PCD User Type	Asset Owner	Probable Uses for Device at UCHC or Other Host Institution for UCHC Residents	Owner of Apps on PCD accessing or storing PHI	PHI Automatically Synched from/to UCHC Clinical Apps	PHI User Entered into Stand Alone PCD Medical Apps (e.g. patient tracker)	Liabile Party for HIPAA Compliance for PHI Of UCHC Patients	Required Data Protections For PCD

Student	UCHC	<ul style="list-style-type: none"> - Synchronization with teaching EMR Software - Enter fictitious patient notes into local PCD software - Enter patient notes with PHI into local PCD software -No interaction with PHI. 	UCHC & Individual Student	Yes, but the EMR used for teaching contains simulated patient data only.	Yes	UCHC if device receives manually entered or automatically fed PHI. No liability exists in patient data is fictitious or device use does not involve PHI.	If device interacts with PHI, then UCHC provides: <ul style="list-style-type: none"> - Strong Authentication - Encrypted PCD Storage - Encrypted transmissions - Device lockout inactivity timer or No liability requires no protections.
----------------	------	---	---------------------------	--	-----	--	---