I. **PURPOSE:**
   A. To outline guidelines which are to be followed to preserve the integrity, privacy, confidentiality and availability of Palomar Health's Information and Information Technology Resources, while allowing employees and authorized non-employees to use technology to carry out job responsibilities and assignments and to further Palomar Health's business objectives.

II. **DEFINITIONS:**
   A. **Availability** - Data or information is accessible and usable upon demand by an authorized person.
   B. **Confidentiality** - Data or information is not made available or disclosed to unauthorized persons or processes.
   C. **Integrity** - Data or information have not been altered or destroyed in an accident or unauthorized manner.
   D. **Information Technology Resources** - Network, Desktop Computers, Mobile/Portable (Devices), Printers, electronic media, magnetic tape, and Removable Storage Devices. A system normally includes hardware, software, information, data, applications, communications, and accounts (system users).
      1. **Mobile/Portable (Devices) Resources** - includes but is not limited to Laptops, Tablets, Pagers, Wireless phones, Palomar Health issued Cellular phones, and any other mobile/portable items/equipment considered as an information technology component.
      2. **Removable Storage Device(s)** - includes but is not limited to USB "Flash" Drives, External Hard Drive, Writeable CD or DVD Drives and any other removable storage items/equipment considered as an information technology component.
   E. **Personally Owned Device(s)** is/are Information Technology Resource(s) that is/are personally-owned. For example, a personal laptop, a personal cellular phone, etc.
   F. **Protected Health Information of PHI** is any individually identifiable health information, in any format, including verbal communications. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes patient billing and health insurance information and applies to a patient’s past, current or future physical or mental health or treatment.
   G. **“Electronic Protected Health Information” or “ePHI”** is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.
   H. **Legal Electronic Signature**: A User's Logon ID and/or Password.
   I. **“Personal Information (PI)”** as used in this policy is an individual’s first name or first initial and last name combined with any one of the following: (1) social security number, (2) driver’s license number or California identification card number, (3) account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account, (4) medical information, or (5) health insurance information.
   J. **“Medical Information”** means any information, in either electronic or physical form, regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor. "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical information and health insurance information for patients are also considered to be PHI.
K. “Restricted Information” (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information.

III. STANDARDS OF PRACTICE:
A. This procedure acts as an extension of the Computer Systems Usage at Palomar Health procedure.
B. All Palomar Health Information Technology Resources as well as the software and data stored, uploaded, downloaded, and transmitted by such devices are property of Palomar Health and are to be protected from unauthorized access, use, modification, destruction or disclosure.

IV. STEPS OF PROCEDURE
A. Security
   1. Palomar Health workforce members shall
      a. Always ensure Palomar Health Information Technology Resource(s) are never left unattended unless physically secured and never left unattended in unsecured areas, including but not limited to a vehicle.
      b. Always take reasonable care of any Palomar Health Information Technology Resource(s) entrusted to you.
      c. Never add or modify any hardware component(s) on any Palomar Health Information Technology Resource(s).
      d. Never add any software to or copy any software off of a Palomar Health Information Technology Resource(s).
      e. Never change the directory structure on Palomar Health Information Technology Resource(s).
      f. Never engage in any activity to disable, uninstall, or compromise Information Technology Resource(s) encryption software.
      g. Never share User IDs and/or Passwords with any other individual and never store them on or near Information Technology Resource(s) in any form.
      h. Use Palomar Health network shared drives for the storage of files, as network shared drives are the only approved location for the storage of Palomar Health files. Never store Palomar Health files on any Mobile Device, Removable Storage Device or on a cloud applications (such as but not limited to Dropbox, Google Cloud, Google Doc, etc)
      i. Always Contact the IT Help Desk at (858) 613-4357
         i. For assistance with storing data to a Palomar Health shared drive, or obtaining a laptop lock.
         ii. To report any problems with any Palomar Health Information Technology Resource(s) and/or software.
      j. Personal Devices should never be used to store Palomar Health information (including but not limited to patient data or other Palomar Health proprietary information).
      k. Always return Palomar Health Information Technology Resource(s) (e.g., PC, Mobile Device(s) and/or Removable Storage Device(s) etc.) to Palomar Health on demand and/or upon termination of employment.
      l. Always Report Lost, Misplaced or Stolen Mobile/Portable and/or Removable Storage Device(s) within 24 hours. Refer to the Information Technology Theft Reporting procedure.

B. End User Agreement
   1. All Palomar Health workforce members will be required upon hire to review this procedure and sign the Mobile/Portable and Removable Storage Device Security and User Agreement form, and to renew it annually.

C. Enforcement
   1. The following occurrences may result in disciplinary action, up to and including termination and/or financial responsibility if it is determined by Palomar Health to be caused by negligence or intentional misuse on the users part.
      a. Damage to Palomar Health Information Technology Resources
      b. Loss of Palomar Health Information Technology Resources.
      c. Violation of applicable laws, including, without limitation, software copyright laws.
      d. Violation of applicable Palomar Health procedures.
e. Failure to follow any provisions of this policy.

D. Exceptions

1. The following outline the exceptions for use of Removable Storage Devices and/or cloud storage.
   a. Palomar Health-issued and approved Removable Storage Devices:
      i. To be considered for approval of a Palomar Health Removable Storage Device(s), workforce members need to complete Removable Storage Device User Request Form and obtain their department Director's signed approval prior to submitting request to Information Security.
      ii. Standard USB "flash" drives issued are encrypted with a storage capacity of 4GB. Any special requests for storage over 4GB or non-encrypted device(s) require additional business justification for increased storage or unencrypted device requirement on the form listed above.
   b. Palomar Health uses Box, considered a cloud storage, as a means to transfer information to business partners when too large to email securely. Email InfoSec@palomarhealth.org to request to be considered for the use of Box.

E. Questions

1. Any questions on this procedure should be referred to the Information Security Office (InfoSec@palomarhealth.org)

V. PUBLICATION HISTORY:

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Effective Date</th>
<th>Document Owner at Publication</th>
<th>Version Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (this version)</td>
<td>06/04/2015</td>
<td>Robin D Ford Manager Info Systems Security</td>
<td>correct link - rdf</td>
</tr>
<tr>
<td>4 (Changes)</td>
<td>06/03/2015</td>
<td>Robin D Ford Manager Info Systems Security</td>
<td>Updated to reflect current practice. ms Reviewed, updated and Approved - rdf</td>
</tr>
<tr>
<td>3 (Changes)</td>
<td>07/08/2014</td>
<td>Robin D Ford Manager Info Systems Security</td>
<td>Review and Update based upon redefined process - rdf</td>
</tr>
<tr>
<td>2 (Changes)</td>
<td>03/07/2014</td>
<td>Robin D Ford Manager Info Systems Security</td>
<td>updated to reflect current practices - ms</td>
</tr>
<tr>
<td>1 (Changes)</td>
<td>01/05/2012</td>
<td>Robin D Ford Manager Info Systems Security</td>
<td>reviewed and approved - rdf</td>
</tr>
<tr>
<td>0 (Changes)</td>
<td>02/04/2011</td>
<td>Luba M Burns</td>
<td>Original procedure to establish guidelines of use for PPH's Information Mobile Resources.</td>
</tr>
</tbody>
</table>

Authorized Signer(s): (06/04/2015) Prudence August, VP, Information Systems

VI. REFERENCES:

<table>
<thead>
<tr>
<th>Reference Type</th>
<th>Title</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referenced Documents</td>
<td>Computer Systems Usage at Palomar Health</td>
<td>Computer Systems Usage at Palomar Health</td>
</tr>
<tr>
<td>Referenced Documents</td>
<td>Information Technology Theft Reporting</td>
<td>Information Technology Theft Reporting</td>
</tr>
<tr>
<td>Referenced Documents</td>
<td>Mobile/Portable and Removable Storage Device Security and User</td>
<td>Mobile/Portable and Removable Storage Device Security and User</td>
</tr>
</tbody>
</table>
Referenced Documents

Agreement
Removable Storage Device User Request

Agreement
Removable Storage Device Security User Agreement

Paper copies of this document may not be current and should not be relied on for official purposes. The current version is in Lucidoc at.

https://www.lucidoc.com/cgi/doc-gw.pl?ref=pphealth:38212$5