Encryption - UMHS Policy 1-04-502 Guide

UMHS Policy 1-04-502 requires all sensitive information to be encrypted. We understand that this will impact operational work flows and have developed this FAQ to help guide you to the appropriate avenue to minimize disruption. Detailed guidance for using removable media can be found here (Level-2 login required).

For a general overview, see this Encryption for Devices document.

<table>
<thead>
<tr>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>Policy Solutions Cheatsheet</td>
</tr>
</tbody>
</table>

Frequently Asked Questions

- **What’s the best way for me to carry data?**
  - If you **must** physically transport data, use an **authorized encrypted flash drive**
  - If you do not need to physically carry the data, use network storage options such as NAS (also known as S:, T:, and H: drives), U-M Box, and MiShare
- **What if I want to store data long term on a flash drive, CD, DVD, or unencrypted hard drive?**
  - All external devices fail, so we recommend using NAS, U-M Box, or other network storage options. We can help you select the best storage for your needs.
- **Where can I get an authorized encrypted flash drive?**
  - Purchase from M-Marketsite (CWD-G Punchout)
  - Purchase from external sites such as Amazon, NewEgg, etc.
  - Removable media drives must meet the NIST FIPS 140-2 standard for HIPAA compliance
- **What if my work requires use of an unencrypted drive?**
  - Fill out an exception request, and detail the reason an exception is necessary. All work with sensitive data requiring use of an unencrypted device must have an approved exception in place. To fill out an exception request, complete the exception form referenced in UMHS Policy 01-04-502 Security of Portable Electronic Devices and Removable Media
- **Who is paying for these drives?**
  - At the present time, there is no funding for these drives
  - Best is to speak to your managers or Chief Department Administrators (CDAs) regarding payment for these drives. Managers have a business obligation to ensure that sensitive data is encrypted.
- **What about my computers or smartphones?**
  - As part of the AirWatch enrollment process, all devices (Windows 10 and Mac computers, iOS, and Android smartphones and tablets) will be encrypted automatically
- **Who can help me?**
  - HITS Service Desk: 734-936-8000 or Submit an Online Request
  - Walk-in Help Me Now service locations at THSL, NCRC, and Towsley
  - Device Support teams can come to your work area

Policy Solutions Cheatsheet