



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



TRANSPORTING PII OR PHI

HIPAA Privacy & Security ♦ April 2010

Background

Each TRICARE Management Activity (TMA) workforce member (whether military, civilian, contractor, or volunteer) is responsible for protecting the personally identifiable information (PII) and protected health information (PHI) of all Department of Defense (DoD) beneficiaries and complying with federal laws such as the Privacy Act of 1974 and the HIPAA Privacy and Security Rules, implemented within the Military Health System (MHS) by appurtenant DoD Regulations including: DoD 5400.11-R, "Department of Defense Privacy Program," DoD 6025.18-R, "DoD Health Information Privacy Regulation," and DoD 8580.02-R, "DoD Health Information Security Regulation." To comply with these laws and regulations, TMA workforce members should apply administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of PII and PHI.

The purpose of this information paper is to provide guidance for transporting PII and PHI, and to provide a sample chain-of-custody template, which can be used by all TMA directorates.

Transportation of PII and PHI

When permitted under DoD regulations, PII and PHI may be physically transported within TMA offices or between approved locations. When transporting PII or PHI between TMA offices, a chain-of-custody log should be used to document any internal transfer of files or electronic media containing PII or PHI. Logs should include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals releasing the information, and other relevant information such as a general description of the information being released.

Appendix A includes a sample chain-of-custody template, which can be customized and used by any TMA directorate.

NOTE: When using the chain-of-custody template in conjunction with PHI, the final documentation must be retained with other HIPAA program documentation and for a period of six years.

When transporting information between approved locations, TMA workforce members should follow the following procedures to ensure that the

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



TRANSPORTING PII OR PHI

HIPAA Privacy & Security ♦ April 2010

confidentiality of PII or PHI is continuously maintained during transport:

- Place all PII or PHI in envelopes or wrappings before transporting it outside of TMA buildings. Envelopes should be able to prevent unintentional disclosure during transit, and should be clearly marked with the originating and destination location information, including at least the name and address of both.

NOTE: The inner documents should be marked “For Official Use Only”. The term "Confidential" is only authorized for use concerning national security classified material in accordance with the provisions of DoD 5200.1-PH, “DoD Guide to Marking Classified Documents.”

- When an individual physically transports PII or PHI between approved locations, the chain-of-custody template should be used.
- Use existing tracking processes that allow a sender and recipient to sign for and verify delivery, such as those associated with FedEx, UPS, and the United States Postal Service.
- If an individual is approved to transport data in physical form during government approved travel, the files must be wrapped in envelopes and properly labeled, and stored in locked carry-on luggage (PII or PHI cannot be a part of checked baggage when traveling).
- If an individual is approved to transport data in electronic portable media form during government approved travel, the data must have appropriate safeguards to ensure adequate protections are in place. Electronic media should be stored in locked carry-on luggage (PII or PHI cannot be a part of checked baggage when traveling).
- Ensure that portable media, when authorized for use, is encrypted and enforce current DoD password standards.
 - Disclose passwords or encryption keys through a different medium, such as a separate e-mail or a phone call, never in notes or documents accompanying the actual media.
- Ensure that transported PII or PHI is delivered only to the appropriate individuals who are authorized to receive such information.

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



TRANSPORTING PII OR PHI

HIPAA Privacy & Security ♦ April 2010

NOTE: An actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII or PHI where unauthorized users gain potential access is known as a breach. Accordingly, once a breach is discovered, there are required remedial actions that must be taken in a prompt manner.

Further information regarding breach response procedures can be found on the TMA Privacy Office Web site at:
<http://www.tricare.mil/tma/privacy/breach.aspx>.

References

- DoD 5200.1-PH, "DoD Guide to Marking Classified Documents," April 1997
- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
- DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
- DoD Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media", July 3, 2007

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041



TRANSPORTING PII OR PHI

HIPAA Privacy & Security ♦ April 2010

TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



Appendix A: Sample Chain-of-Custody Template

Chain-of-Custody Documentation

<Date>

Description of items: <>

<p>Original Recipient</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Organization/Directorate: _____</p> <p>Address: _____</p> <p>Address: _____</p> <p>City, State, ZIP Code: _____</p> <p>Phone Number: _____</p> <p>Date and Time of Receipt: _____</p>	<p>Custody Transfer 1</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Organization/Directorate: _____</p> <p>Address: _____</p> <p>Address: _____</p> <p>City, State, ZIP Code: _____</p> <p>Phone Number: _____</p> <p>Date and Time of Receipt: _____</p>
<p>Custody Transfer 2</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Organization/Directorate: _____</p> <p>Address: _____</p> <p>Address: _____</p> <p>City, State, ZIP Code: _____</p> <p>Phone Number: _____</p> <p>Date and Time of Receipt: _____</p>	<p>Custody Transfer 3</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Organization/Directorate: _____</p> <p>Address: _____</p> <p>Address: _____</p> <p>City, State, ZIP Code: _____</p> <p>Phone Number: _____</p> <p>Date and Time of Receipt: _____</p>