HealthPartners®

ORGANIZATIONAL PRIVACY STANDARDS:

# Sending Protected Information Securely

**Definitions**:

**De-Identified Information** means information about a member or patient that is not Protected Information because it does not identify the individual and does not contain sufficient information to reasonably allow someone to figure out who the patient or member is. For information to be considered De-Identified, it must follow the standards for de-identification established in HIPAA. You should not assume that just because a name is not attached to the information that it is De-Identified Information. To determine if information is truly, legally De-Identified, consult with the Law Department or the Office of Integrity and Compliance.

**Encrypted Information** means Protected Information that has been electronically masked or otherwise made unviewable and unalterable by anyone who does not have a code, key, password or decryption technology to allow viewing.

**Basic Rules:**

1. All Protected Information must be transmitted (sent outside the organization) in accordance with the organization's Privacy and Security Policies and Privacy and Security Standards.

2. Whenever possible to accomplish the assigned task, transmit De-Identified Information.

3. If any of the data elements listed below are associated with the information you are transmitting, then it is *highly* likely that the information is Protected Information and so subject to specific transmission requirements discussed below:
   - Name
   - Address
   - Five-digit zip codes
   - Telephone or fax number
   - Email address
   - Social security number
   - Medical record or insurance ID number
   - Driver's license number or other vehicle or professional license number
   - Medical device identifier or serial number
   - Biometric identifiers, including fingerprints, voice codes, retinal scans or DNA
   - Photographic images that contain identifying marks or characteristics
   - Date of Birth

4. When transmitting Protected Information outside the organization, you are permitted to transmit only the amount and kind of Protected Information that is reasonably required to accomplish the assigned task. That means:

- To support **treatment**, use your best professional judgment as to what kind and how much of the patient's information you need to transmit;
- To support **payment-related activities** or **health care operations,** start with De-Identified information and piece by piece add identifiable information until you have the information you actually need to accomplish the task – and then transmit only that information.

5. When transmitting electronic Protected Information outside the organization, you must use one of the five (5) **secure transmission methods** listed below.

6. **Secure Transmission Methods**: The table below identifies secure methods for transmitting electronic Protected Information that conform to the organization's Privacy and Security Policies and Standards. For assistance accessing or using any of these options, contact IS&T Security Management.

| Method | Description | Limitations | User Guidance |
|---|---|---|---|
| **1. Secure Mail** | • Point-to-point email distribution<br>• Secure envelope mail delivery | • Would not prevent unauthorized disclosure if email sent to wrong address<br>• 10MB maximum file size | • Use for small files that will typically only be sent to one recipient and contain limited Protected Information.<br>• **Always** verify the recipient email address before sending the message. |
| **2. E-Transfer** | • Encrypts data<br>• Handles larger files | • Requires separate communication of User ID and Password<br>• 200MB maximum file size | • Use for medium sized files that will typically only be sent to one recipient.<br>• **Always** send the User ID and Password to the recipient via a separate transmission method.<br>• **Always** verify the recipient email address before sending the messages. |

# Sending Protected Information Securely

| Method | Description | Limitations | User Guidance |
|---|---|---|---|
| **3. PointSec Portable Media Encryption** | • Encrypts portable media (CDs, flash drives) | • Requires separate communication decryption key | • Use when recipient of the data requires physical media.<br>• **Always** send the decryption key to the recipient via a separate transmission method. |
| **4. Encrypted Processes Employed by the HealthPartners EDI Business Unit** | • Encrypts the "envelope" and/or "tunnel"<br>• Set-up is tested to ensure the connection is correct<br>• Handles any size files<br>• Transmission can be scheduled | • Requires coordination of audit process to ensure data is not sent in the incorrect "envelope"<br>• Requires lead time to set-up connections<br>• Requires coordination with our customers | • Recommended for files that are sent on a routine schedule.<br>• Business units and IS&T should coordinate an automated audit function that validates and ensures that the correct data is entered into the correct "envelope."<br>• For ad hoc or urgent requests, incorporate additional validation points. |
| **5. Portals** | • Encrypts the "tunnel"<br>• Set-up is tested to ensure the connection is correct<br>• Handles large files<br>• IS&T can configure so that recipient "pulls" data from a secure web environment.<br>• Examples include Provider Portal, Online Patient Services and HealthPartners.com Secure Messaging. | • Requires coordination with our customers<br>• Requires lead time to set-up connections<br>• Requires modification to current reporting methods | • Modify reporting process so that customer "pulls" data, rather than our pushing the information to a mailbox.<br>• Use whenever possible for sharing Protected Information with employers, brokers and providers. |

**Exceptions:**

There are only limited exceptions to the requirements for transmitting Protected Information outside the organization as described in this standard, and those will depend on the circumstances. If you are considering transmitting Protected Information in a manner that is not described in this standard, you must first consult with IS&T Security Management.

**Important Reminder:**

These are important standards for you to follow. If you don't follow them, you may be subject to discipline.

**Resources:**

*Organizational Privacy Standards:* Minimum Necessary
*Organizational Privacy Standards:* Protected Information, De-Identified Information and Encrypted Information
*Organizational Privacy Standards:* Using E-Mail to Communicate With and About Patients and Members
*Organizational Privacy Standards:* Business Associates and Business Associate Agreements