



**Form PF-6000
HIPAA FORM FOR
RECORDS DESTRUCTION**



OFFICE NAME: _____
OFFICE ADDRESS: _____
PHYSICIAN NAME(S): _____

CERTIFICATE OF DESTRUCTION: The information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures. (Adult records should be retained for 10 years from last visit. Pediatric patient records are to be kept 10 years or until patient is 21 years of age., whichever is longer.

Date of Destruction:	Authorized By:
Description of Information Disposed Of/Destroyed:	
Inclusive Dates Covered:	

METHOD OF DESTRUCTION:

- PURGING OF ELECTRONIC DATA (EMR)
- Burning
- Overwriting
- Pulping
- Pulverizing
- Reformatting
- Shredding
- Other: _____

Records Destroyed By*:
If On Site, Witnessed By:
Department Manager:

**If records destroyed by outside firm, you must confirm a contract exists*

AUTHORIZED BY PHYSICIAN (Print Name: _____

SIGNATURE OF PHYSICIAN: _____ DATE: _____

HIPAA

Information Safety Management Program

PRIVACY & SECURITY

POLICIES & PROCEDURES

P-7575 Destruction/disposal of protected health information

Policy

It is the policy of the ProHealth Partners/Argus Medical Management to ensure the privacy and security of protected health information in the maintenance, retention and eventual destruction/disposal of such media. Destruction/disposal of protected health information will be carried out in accordance with federal and state law, state policy and as defined in our retention policy. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit or litigation. Retention of records for adults will be for 10 years past the last date of service. Pediatric medical records should be retained for 10 years or until the patient is 21 years of age, whichever is longer.

Definitions

Protected Health Information/Media:

- Any record of an individual's health information, regardless of medium or characteristic that can be retrieved at any time.
 - This includes all original consumer records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting consumer care or business.

Procedures

- All destruction/disposal of protected health information media will be done in accordance with federal and state law, state policy and following written retention policy/ schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.

- Records or other documents containing protected health information scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of consumer information is complete. This means that this material should be stored in secure containers (not in wastebaskets, boxes, recycle bins, etc.) until the time of destruction/disposal.

- Contracts between physician(s) and business associates will provide that, upon termination of the contract, the business associate will return or destroy/dispose of all consumer health information. The destruction of protected health information by the Business Associate will be documented in writing and sent to the physician office and are to include:
 - Date of destruction/disposal.
 - Description of the destroyed/disposed record series or medium.
 - Method of destruction/disposal.
 - Inclusive dates covered.
 - A statement that the consumer information records were destroyed/disposed of in the normal course of business.
 - The signatures of the individuals supervising and witnessing the destruction/disposal.
- If such return or destruction/disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/ disposal.

- A record of all case files containing protected health information that are destroyed or disposed will be made and retained permanently by physician(s). Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the consumer information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:
 - Date of destruction/disposal.
 - Method of destruction/disposal.
 - Description of the destroyed/disposed record series or medium.
 - Inclusive dates covered.
 - A statement that the consumer information records were destroyed/disposed of in the normal course of business.
 - The signatures of the individuals supervising and witnessing the destruction/disposal.

- If destruction/disposal services are contracted or performed by another state agency, the contract or agreement will provide that physician(s) business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law and include the following elements:
 - Specify the method of destruction/disposal.
 - Specify the time that will elapse between acquisition and destruction/disposal.
 - Establish safeguards against breaches in confidentiality.
 - Indemnify physician(s) from loss due to unauthorized disclosure.
 - Require that a non-state government business associate maintain liability insurance in specified amounts at all times the contract is in effect.
 - Provide proof of destruction/disposal.

Consumer information media will be destroyed/disposed of using a method that ensures the consumer information cannot be recovered or reconstructed. Methods of destruction/disposal may be reassessed annually by the security officer, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

Procedures: Disposal of Internal Electronic Protected Health Information (E PHI)

1. Disposal of Internal Electronic Protected Health Information

Purging of electronic health information will follow all policies and procedures required by federal and state regulations. Physicians will sign authorization form authorizing purging of patient data and billing electronic records from the EMR, Practice Management and Billing system.

Procedures: Disposal of External Media / Hardware

2. Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information (“PHI”) or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.
- Destruction of External Media shall be logged, and witnessed by Security IT Officer.

2. Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

3. Disposition of Excess Equipment

As the older Practice computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

P-8000 Resolution of Complaints and Breaches

The **Privacy Officer** will implement the procedures established in policies P-8100 through [P-8400](#) by which a patient or other individual may file a complaint concerning the privacy policies and procedures that have been adopted by **ProHealth Partners**, or the compliance of staff with those policies.

The **Privacy Officer** also will implement the procedures established in policy [P-8400](#) to mitigate the harmful effect of uses or disclosures of protected health information that violate the privacy policies and procedures established by this manual.