

Policy & Procedure



HIPAA / PRIVACY PREFACE

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

Long-term care facilities have a long-standing commitment to protecting the privacy of patient health information which is sometimes referred to as Protected Health Information ("PHI"). A part of this commitment involves compliance with the privacy standards contained in the regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the first comprehensive federal protection of health information. The regulation is known as the Privacy Rule.

The following is a general overview of the requirements of the HIPAA privacy regulations. Each facility is referred to as a "Covered Entity" by these regulations and in this statement.

The HIPAA regulations govern the use and disclosure of PHI. In general, a Covered Entity may use PHI for purposes of treatment, payment, and health care operations. It may disclose PHI

1. With the individual's authorization;
2. To another healthcare provider for treatment and payment purposes with the individual's authorization; and
3. In certain other circumstances described by the regulations.

In using or disclosing PHI a Covered Entity must restrict the use or disclosure to the minimum amount necessary to accomplish the purpose of the use or disclosure. Employees of a Covered Entity will be assigned classifications that will determine the employees' access to PHI in order to comply with the minimum necessary requirement.

The HIPAA regulations also give individuals several rights with respect to their PHI. In addition to the rights to have access and to receive confidential communications about PHI, the individual may copy and inspect PHI, restrict its use and disclosure, amend it, and receive an accounting of disclosures made of their PHI.

There are many obligations imposed on a Covered Entity by the privacy regulations. These

- Include developing and implementing policies and procedures to assure compliance;
- Training members of its workforce in the HIPAA requirements appropriate to their jobs;
- Documenting its efforts to achieve compliance; developing and implementing safeguards to protect PHI; and
- Designating a Privacy Official.

A Privacy Official is an individual designated by the Covered Entity who is responsible for the development and implementation of the required policies and procedures for compliance with HIPAA. The Covered Entity must also designate a person, who may be the Privacy Official, to handle complaints and to provide information about the entity's practices with respect to PHI.



Policy & Procedure

HIPAA / PRIVACY
PREFACE

FUNCTION HIPAA
NUMBER 1000
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

The Covered Entity must state its practices with respect to the use and disclosure of PHI, the individual's rights and the Covered Entity's obligations in a "Notice of Privacy Practices". This Notice must be given to individuals at the time the treatment relationship begins.

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION
HIPAA

NUMBER
1000

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

A

Accounting of Disclosures –

A log that is maintained for each resident that indicates the disclosures that have been made of his or her PHI.

Active Medical Record –

The active Medical Record consists of two parts: (1) the active record which is filed at the nurses' station/active record storage area and (2) the overflow files. (See also Medical Record.)

Administrative Tribunal –

A judge or group of judges who conduct hearings and exercise judgment over specific issues involving persons or things.

Administrative – connotes of or pertains to administration, especially management, as by managing or conducting, directing or superintending the execution, application, or conduct of persons or things.

Tribunal – is the seat of a judge; the place where he administers justice. The whole body of judges who compose a jurisdiction; a judicial court; the jurisdiction that the judges exercise.

Alternative Communication Means –

Information or communications delivered to residents by the practitioners in a manner different than the normal practice of the practitioner. For example, the resident may ask for delivery at an alternative address, phone number or post office box; or that discussion of PHI be limited when specified people are present.

Amend / Amendment –

An amendment to PHI will always be in the form of information *added to* the existing PHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial PHI more precise, or show some of the original PHI to be incorrect. However, the original PHI is never altered. Changes are indicated by the addition of the amended information.

Authorization –

A resident's statement of agreement to the use or disclosure of Protected Health Information to a third party.

B

Business Associate (BA) –

A person or organization that performs a function or an activity on behalf of the Pinnacle Health Management that involves the use or disclosure of Protected Health Information. A business associate might also be a person or entity that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services involving the use or disclosure of PHI.

C

CMS – Centers for Medicare and Medicaid Services –

The agency formerly known as HCFA (Health Care Financing Administration) that regulates and enforces Federal Regulations for Medicare in Long Term Care and other health care entities.

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

Conditioned –

An authorization is “conditioned” if a resident cannot obtain treatment or service unless he or she signs that authorization.

Continuum of Care –

A range of services available to people in the community. They include supportive, rehabilitative, preventive and social services. They meet various levels of need or impairment.

Court Order –

An order issued from a competent court that requires a party to do or abstain from doing a specific act.

Covered Entity –

A health care provider who transmits health care information using one of the transaction standards defined by the Department of Health and Human Services. An example of this would be billing Medicare and Medicaid electronically for services Pinnacle Health Management provides to a resident.

D

De-Identification –

The process of converting individually identifiable information into information that no longer reveals the identity of the resident. Information may be de-identified by statistical de-identification or the safe harbor method of de-identification.

De-Identified Health Information –

Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

Department of Health and Human Services (HHS) –

The federal agency charged with the development, statement and implementation of the HIPAA Privacy Rule.

Designated Record Set –

Resident Medical Records and billing records maintained and used by the practitioner to make decisions about the resident. In this context a record is any item, collection, or grouping of information that contains Protected Health Information and is maintained, collected, used or disclosed by the practitioner. The Designated Record Set also includes billing information that may contain ICD-9-CM codes that represent health conditions of the resident and that are part of the resident’s Protected Health Information.

For access to the Designated Record Set, the State Operations Manual [SOM] (F153) allows the resident to “have access to all records pertaining to him or her including current clinical records.” The Guidance to Surveyors indicates that the term “records” includes “all records pertaining to the resident such as trust fund ledgers pertinent to the resident and contracts between the resident and the practitioner.”

The SOM (F164) further defines personal records in the Guidance to Surveyors to include all types of records Pinnacle Health Management might keep on a resident, whether they are medical, social, fund accounts, automated or other.

Directory Information –

The three pieces of information that are considered “Directory Information” include:

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- Resident name
- Condition described in general terms (e.g., "He is not feeling well." or "She is having a good day.")
- Religious affiliation (available only to members of the clergy)

Disclosure –

To release, transfer, provide access to or divulge in any way a resident's health information to individuals or entities outside of Pinnacle Health Management. (See also Use.)

Routine Disclosure – Customary disclosures of PHI that Pinnacle Health Management discloses on a regular basis.

Non-Routine Disclosure – Disclosures of PHI that are not usually disclosed by Pinnacle Health Management.

E F

Financial Records –

Admission, billing, and other financial information about a resident included as part of the Designated Record Set.

Fundraising –

An organized campaign by a private, non-profit or charitable organization designed to reach out to certain segments of the population or certain identified populations in an effort to raise monies for their organization or for a specific project or purpose espoused by their organization.

G H

Health Care Operations –

Any of the following activities of Pinnacle Health Management:

1. Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting of health care providers and residents with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating employee and practitioner performance, conducting training programs under supervision to practice or improve skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development such as conducting cost-management and planning related analyses related to managing and operating Pinnacle Health Management;

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

5. Business management and general administrative activities of Pinnacle Health Management, including, but not limited to:
- Customer service
 - Resolution of internal grievances
 - Due diligence in connection with the sale or transfer of assets to a potential successor in interest
 - Creating de-identified health information, fundraising for the benefit of Pinnacle Health Management and marketing for which an individual's authorization is not required.

Health Care Provider –

An entity that provides health care, service or supplies related to the health of an individual, e.g., medical, dental, physical therapy, or chiropractic clinics; hospitals, etc.

HIPAA –

Refers to the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996, in particular the portion of the Act known as Administrative Simplification (Subpart F) dealing with the privacy of individually identifiable health information.

I

Individually Identifiable Health Information (IIHI) –

Any information, including demographic information, collected from an individual that:

1. Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
2. Relates to the past, present or future physical or mental health or condition of an individual, and
 - a. Identifies the individual or
 - b. With respect to which there is reasonable basis to believe that the information can be used to identify the individual.

Institutional Review Board (IRB) –

In reference to a research project, a board that is designated to review and approve proposed research and the process by which the investigator intends to secure the informed authorization of participants.

L

Limited Data Set (LDS) –

A data set that includes elements such as dates of admission, discharge, birth and death as well as geographic information such as the five digit zip code and the individual's state, county, city or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

M

Marketing –

1. To provide information about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- a. To describe a health-related product or service (or payment for such product or service) that is provided by or included in a plan of benefits of the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancement to, a health plan; and health-related products or services available only to a health plan enrollee that add values to, but are not part of, a plan of benefits;
 - b. For treatment of that individual; or
 - c. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual.
2. An arrangement between a covered entity and any other entity whereby the covered entity discloses Protected Health Information to the other entity in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Medical Record: -

The collection of documents, notes, forms, test results, etc. which collectively document the health care services provided to an individual in any aspect of health care delivery by a provider; individually identifiable data collected and used in documenting healthcare services rendered. The Medical Record includes records of care used by healthcare professionals while providing resident care services, for reviewing resident data, or documenting observations actions or instructions. The Medical Record is included as part of the Designated Record Set.

Minimum Necessary –

The least amount of Protected Health Information needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of Protected Health Information it uses, discloses or requests to the minimum necessary to do the job.

N

Notice of Privacy Practices –

A document required by HIPAA that provides the resident with information on how the Facility generally uses a resident's Protected Health Information and what the resident's rights are under the Privacy Rule.

O

Office of Civil Rights –

The agency with the U.S. Department of Health and Human Services that has responsibility for enforcement of the HIPAA Privacy Rule. (www.usda.gov/cr/)

Opt Out –

To make a choice to be excluded from services, procedures or practices. Resident rights under HIPAA include many situations where the resident may request to be excluded from a service, procedure or practice. In most cases, the Facility must comply or attempt to comply with the request to be excluded.

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION
HIPAA

NUMBER
1000

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

P

Payment –

The activities undertaken by a health care provider or payer to obtain reimbursement for the provision of health care.

Personal Representative –

Is the term used in the Privacy Rule to indicate the person who has authority under law to act on behalf of a resident. *For purposes of the Privacy Rule a Facility must treat a personal representative as having the same rights as the resident unless there is a reasonable belief that the personal representative has subjected the resident to abuse or neglect, or treating the person as the personal representative could endanger the resident.*

Policy –

A high-level over-all plan embracing the general principles and aims of an organization.

Pre-emption / Pre-empts –

Taking priority over or supercedes.

Privacy Breach –

A violation of one's responsibility to follow privacy policy and procedure that results in the residents' PHI being accessed by unauthorized persons.

Privacy Official –

The person in Pinnacle Health Management who is the designated point of contact for HIPAA-related issues and whose position includes oversight of training related to HIPAA. May also be called the Privacy Representative or the HIPAA Point of Contact (HPOC).

Privacy Officer –

The person designated by the organization who is responsible for development and implementation of the HIPAA policies and procedures. The Privacy Officer serves as a resource to assist each Pinnacle Health Management's Privacy Official in implementing HIPAA policies and procedures. HIPAA requires that each covered entity appoint a Privacy Official

Privacy Rule –

Refers to the regulation issued by the Department of Health and Human Services entitled Standards for Privacy of Individually Identifiable Health Information that was published on December 28, 2000, and subsequently modified on August 14, 2002. The effective date for the Privacy Rule is April 14, 2003. In this Policy and Procedure Manual, "HIPAA" and "Privacy Rule" are used interchangeably.

Protected Health Information (PHI) –

Information that is a subset of health information, including demographic information, and:

1. Is created or received by a health-care provider, health plan, employer or health-care clearinghouse; and

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - a. That identifies the individual; or
 - b. There is a reasonable basis to believe the information can be used to identify the individual.

Psychotherapy Notes –

Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes must be kept separate from the rest of the resident's Medical Record.

Q

Qualified Protective Order –

A legal command intended to protect a person or thing from an unfair or unjust action.

Order – a mandate, precept; a command or direction authoritatively given; a rule or regulation.

R

Re-Identification –

The process of converting de-identified health information back to individually identifiable health information. Re-identified health information does reveal the identity of the resident and must be treated as PHI under the HIPAA Privacy Rule.

Research –

A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

Resident –

As used in this Manual includes patient.

Revoke –

To cancel or withdraw an authorization to release medical information.

Role Based Access –

Access to PHI based on the duties of employees. Pinnacle Health Management will identify persons or classes of persons in its workforce who need access to PHI to carry out their duties and make a reasonable effort to limit access PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

S

Safeguarding –

To ensure safekeeping of Protected Health Information for the resident.

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

Security Officer –

A position mandated by the HIPAA. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation.

State Operations Manual (SOM) –

Federal Regulations that govern all Skilled Nursing Facilities that receive federal funding from Medicare and/or Medicaid.

Subpoena (2 Kinds) –

A process to cause a witness to appear and give testimony, commanding him to lay aside all pretenses and excuses, and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof.

Duces Tecum –A request for witnesses to appear and bring specified documents and other tangible items. The subpoena *duces tecum* requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.

General Subpoena (AKA Ad Testificandum) –A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

T

TPO –

(See Treatment, Payment and Operation.)

Treatment –

The provision, coordination or management of health care and related services by the practitioners, including the coordination or management of health care by the Pinnacle Health Management with a third party; consultation with other health care providers relating to a resident; or the referral of a resident for health care between the Pinnacle Health Management and another health care provider.

Treatment, Payment and Operations (TPO) –

The Privacy Rule allows sharing of information for purposes of treatment, payment and health care operations. Treatment includes use of resident information for providing continuing care. Payment includes sharing of information in order to bill for the care of the resident. Health care operations are certain administrative, financial, legal, and quality improvement activities that are necessary for Pinnacle Health Management to run its business and to support the core functions of treatment and payment.

U

Use –

To share, apply, use, examine or analyze health information within Pinnacle Health Management. (See also Disclosure).

Policy & Procedure



HIPAA / PRIVACY GLOSSARY

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

V W

Whistleblower –

A person, usually a staff member, who reveals wrongdoing within an organization to the public, government agencies or to those in positions of authority.

Workforce –

Employees, volunteers, trainees and other persons whose conduct, in the performance of work for Pinnacle Health Management, is under the direct control of Pinnacle Health Management, whether or not they are paid. Members of the workforce are not business associates.

Policy & Procedure



HIPAA / PRIVACY SAFEGUARDING

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information (“PHI”) by Pinnacle Health Management and to limit unauthorized disclosures of PHI that is contained in a resident’s Medical Record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of the resident.

POLICY

The intent of this policy is to ensure, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal or state regulation governing confidentiality and privacy of health information. The following procedure is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is, or will be, contained in a resident’s Medical Record.

PROCEDURE

Pinnacle Health Management Privacy Official and Administrator, who is the Managing Partner, shall periodically monitor Pinnacle Health Management’s compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by Pinnacle Health Management, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:

1. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
2. Meetings will be conducted in a room with a door that closes, if possible.
3. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.
4. Only staff members who have a “need to know” the information will be present at the meeting. (See the Policy “Minimum Necessary Uses and Disclosures.”)
5. The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

Telephone conversations:

1. Telephones used for discussing PHI are located in as private an area as possible.
2. Staff members will take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
 - a. Lowering the voice

Policy & Procedure



HIPAA / PRIVACY SAFEGUARDING

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- b. Requesting that unauthorized persons step away from the telephone area
 - c. Moving to a telephone in a more private area before continuing the conversation
3. PHI shared over the phone will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

In-Person conversations:

- In resident rooms
- With resident/family in public areas
- With authorized staff in public areas

Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:

1. Lowering the voice
2. Moving to a private area within the Facility
3. If in resident room, pulling the privacy curtain

Safeguards for Written PHI

All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.

Active and Inactive Business Office Files:

1. Active and inactive Business Office Files which included copies of clinician's reports shall be stored electronically in a secure area that allows only authorized staff access as needed.
2. In the event that the confidentiality or security of stored PHI has been breached, Pinnacle Health Management Privacy Official and Administrator shall be notified immediately.
3. In the event of a change in ownership of Pinnacle Health Management, the Medical Records shall be maintained as specified in the Purchase and Sale Agreement.

PHI Not a Part of the Designated Record Set:

1. Use of "shadow" charts or files is discouraged.
2. Any documentation of PHI shall be stored in a location that ensures, to the extent possible, that such PHI is accessible only to authorized individuals.
3. All PHI created by the clinician shall be filed in the Facility Medical Record. The copy of each report is to either be scanned and emailed, faxed or mailed to the Business Office. Once transmission has been completed the shadow copy will be destroyed in accordance with 1018. *Destruction of PHI.*

Policy & Procedure



HIPAA / PRIVACY SAFEGUARDING

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

Office Equipment Safeguards

Computer access:

1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
2. All users of computer equipment must have unique login and passwords.
3. Passwords shall be changed every 90 days.
4. Posting, sharing and any other disclosure of passwords and/or access codes is **strongly discouraged**.
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.
6. Facility based staff members shall log off their workstation when leaving the work area.
7. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.
8. Employee access privileges will be removed promptly following their departure from employment.
9. Employees will immediately report any violations of this Policy to their supervisor, Administrator or Facility Privacy Official.

Printers, copiers and fax machines:

1. Printers will be located in areas not easily accessible to unauthorized persons.
2. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. Sample language: "Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc). Access to such documents by unauthorized persons is prohibited by federal law."
3. Documents containing PHI will be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.
4. Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or, in a Facility setting, by placing the document in a secure shredding bin until destroyed.

Policy & Procedure



HIPAA / PRIVACY SAFEGUARDING

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

Destruction

Written:

Documentation that is not part of the Medical Record and will not become part of the Medical Record (e.g., report sheets, shadow charts or files, notes, lists of vital signs, weights, etc.) shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

Electronic:

Prior to the disposal of any computer equipment, including donation, sale or destruction, Pinnacle Health Management must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.

(See the Policy "Destruction of Protected Health Information" for additional guidelines.)

Policy & Procedure



HIPAA / PRIVACY USE AND DISCLOSURE

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To provide guidance on the use and/or disclosure of Protected Health Information (“PHI”) for research purposes.

POLICY

Pinnacle Health Management must obtain a resident's authorization before releasing his/her PHI for research purposes.

Pinnacle Health Management will ensure that an appropriately instituted and formally designated (per Federal Drug Administration/FDA regulations) Institutional Review Board is utilized for the protection of human subjects in any research activity involving access to PHI under Pinnacle Health Management's control.

The resident has the right to refuse to participate in research. (See *F155* in the State Operations Manual.)

Pinnacle Health Management shall abide by the experimental subject's (resident's) privacy rights.

PROCEDURE

1. Federal regulations and state laws regulate the use of human subjects (residents) in any investigation designed to develop or contribute to specific knowledge. Such laws require that specific information be disclosed so that a subject (resident) may give informed authorization and that authorization must be documented.
 - a. At the beginning of any research project, Pinnacle Health Management and the entity involved in the research must determine and agree on who will be responsible for obtaining an authorization to use or disclose PHI.
 - b. If an outside authorization is utilized, Pinnacle Health Management Privacy Designee will review the resident's authorization to assure that it is valid in accordance with the HIPAA Privacy Rules and those special provisions related to research. (See Policy “Authorization for Release of Protected Health Information.”)
 - c. Special Authorization Provisions Related to Research
 - i. Expiration Date: The *Authorization* form will state the expiration date or that the expiration event is “end of research study,” “none,” or similar language.
 - ii. Combining Authorization: The *Authorization* form may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research.

Policy & Procedure



HIPAA / PRIVACY USE AND DISCLOSURE

FUNCTION

HIPAA

NUMBER

1000

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- iii. Condition Treatment on Authorization: The provision of research-related treatment may be conditioned on the provision of an authorization for the use or disclosure of PHI for such research.
2. Federal law requires the establishment of an Institutional Review Board (“IRB”) to review and approve proposed research and the process by which the investigator intends to secure the informed authorization of participants.
 - a. Institutions engaged in research involving human subjects (e.g., medical schools, universities, large hospitals) will usually have their own IRB to oversee research conducted within the institution or by staff of the institution.
 - b. It is the responsibility of the organization or institution conducting the research to establish or contract with an IRB; it is Pinnacle Health Management’s responsibility to ensure that an IRB is utilized.
3. If the research study is approved by the IRB and de-identified health information can be used or disclosed, then no further privacy implications exist. (See the Policy “De-Identification of Protected Health Information” for details of how to de-identify the health information for disclosure.)
4. If the research study is approved by the IRB and de-identified health information cannot be used or disclosed, then an *Authorization* form is required and must be obtained from each resident included in the research study.
5. Appropriate Facility staff will manage requests to participate in research studies and coordinate the review process by the IRB.
 - a. Contact/communications with the IRB and related findings must be documented and communicated to Pinnacle Health Management Privacy Designee.
 - b. If Pinnacle Health Management participates in research projects, Pinnacle Health Management Privacy Designee must have a method of tracking the correspondence, decisions and other communications regarding the research project.
6. Pinnacle Health Management will inform every resident of any research or economic interest (for example, any direct or indirect remuneration that may come to Pinnacle Health Management as a result of the research) that may result from his or her treatment.
7. Pinnacle Health Management or the entity conducting the research will obtain the resident’s *Authorization* form when required. (See Item 1.)
8. Pinnacle Health Management Privacy Designee will file the original copy of the request and the associated response in the participant’s Medical Record.

Policy & Procedure



HIPAA / PRIVACY EMAIL PHI

FUNCTION
HIPAA

NUMBER
1000

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

PURPOSE

To ensure the appropriate use of the email system when transmitting Protected Health Information ("PHI").

POLICY

It is the policy of Pinnacle Health Management to protect the electronic transmission of PHI as well as to fulfill our duty to protect the confidentiality and integrity of resident PHI as required by law, and professional ethics. The information released will be limited to the minimum necessary to meet the requestor's needs. Whenever possible, de-identified information will be used.

PROCEDURE

1. E-mail users shall use a unique identity complete with unique password and file access controls.
2. E-mail users may not intercept, disclose or assist in intercepting and disclosing e-mail communications.
3. Resident specific information regarding highly sensitive health information must not be sent via e-mail, even within the internal email system (i.e. information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
4. Users will restrict their use of email for communicating normal business information such as information about operational and administrative matters, such as billing.
5. Users should verify the accuracy of the email address before sending any PHI and, if possible, use email addresses loaded in the users address book.
6. PHI may be sent unprotected via e-mail within a properly secured, internal network of the organization. When sending PHI outside of this network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information. Sample security measures include password protecting the document(s) being sent or encrypting the message.
7. All e-mail containing PHI will contain a confidentiality statement (see sample below).
8. Users should exercise extreme caution when forwarding messages. Sensitive information, including resident information, must not be forwarded to any party outside the organization without using the same security safeguards as specified above.
9. Users should periodically purge e-mail messages that are no longer needed for business purposes, per the organization's records retention policy.
10. Employee e-mail access privileges will be removed promptly following their departure from the organization.

Policy & Procedure



HIPAA / PRIVACY EMAIL PHI

FUNCTION
HIPAA

NUMBER
1000

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

11. Email messages, regardless of content, should not be considered secure and private. The amount of information in any email will be limited to the minimum necessary to meet the needs of the recipient.
12. Employees should immediately report any violations of this guideline to their supervisor, Administrator or Privacy Official.

Sample Confidentiality Statement

The information contained in this e-mail is legally privileged and confidential information intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any viewing, dissemination, distribution, or copy of this e-mail message is strictly prohibited. If you have received and/or are viewing this e-mail in error, please immediately notify the sender by reply e-mail, and delete this e-mail from your system. Thank you.

Policy & Procedure



HIPAA / PRIVACY RESPONDING TO A SUBPOENA

FUNCTION

HIPPA

NUMBER

1004

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To ensure that Pinnacle Health Management complies with HIPAA Privacy Rule requirements when a subpoena requesting Protected Health Information (“PHI”) is served.

POLICY

Protected Health Information may be disclosed pursuant to judicial or administrative process without the written authorization of the resident, or the opportunity for the resident to agree or object, subject to certain conditions. Pinnacle Health Management will disclose PHI in the course of judicial or administrative process in response to a court or administrative tribunal order. Pinnacle Health Management will disclose PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order, subject to the conditions set forth in this procedure. In either case, **Pinnacle Health Management will disclose only that PHI expressly authorized by the subpoena, discovery request, other lawful process, or court order.** (Pinnacle Health Management may contact its legal counsel to review and verify the legality of a subpoena requesting PHI served.)

PROCEDURE

1. If the subpoena or other lawful request is accompanied by an order of a court or administrative tribunal, Pinnacle Health Management will verify the identity and authority of the individuals requesting PHI.
2. If the order of the court or other administrative tribunal is valid and meets the verification requirements, Pinnacle Health Management will disclose only that PHI expressly authorized by such order.
3. If the subpoena, discovery request or other lawful process (“subpoena”) is not accompanied by a court order, Pinnacle Health Management will disclose the PHI only after obtaining satisfactory assurances from the party seeking the information that they have made reasonable efforts
 - a. To notify the individual who is the subject of the requested PHI, or
 - b. To secure a qualified protective order.
4. **Notice to individual.** Prior to disclosing PHI when the subpoena is not accompanied by a court order and there is no qualified protective order meeting the requirements of the Privacy Rule, Pinnacle Health Management will obtain a written statement and accompanying documentation from the requesting party that meets all of the following requirements:
 - a. The written statement and documentation must demonstrate that reasonable efforts have been made to give notice of the request to the individual who is the subject of the requested PHI.

Policy & Procedure



HIPAA / PRIVACY RESPONDING TO A SUBPOENA

FUNCTION

HIPPA

NUMBER

1004

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- b. The notice must contain sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal.
- c. The written statement and accompanying documentation must demonstrate that:
 - i. Time for raising objections to the court or administrative tribunal has elapsed, and
 - ii. No objections were filed, or
 - iii. The court has resolved all objections filed by the individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.
5. Qualified Protective Order. A qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
 - a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
 - b. Requires the return to Pinnacle Health Management or destruction of the PHI, (including all copies made) at the end of the litigation or proceeding.
6. Prior to disclosing PHI when the subpoena is not accompanied by a court order and the above notice requirements are not met, Pinnacle Health Management will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
 - a. The parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or
 - b. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
7. If the requesting party is unable to meet the requirements for Notice or a Qualified Protective Order, Pinnacle Health Management will notify the requesting party that it is unable to comply with the subpoena. (See "Response to a Subpoena" letter following this Policy.)
8. If the requesting party decides to pursue the request for the PHI without meeting the above requirements, Pinnacle Health Management's Privacy Official will contact Pinnacle Health Management's Legal Counsel for further direction.
9. Pinnacle Health Management's Privacy Official shall document the information regarding the subpoena or other legal process that requests PHI in an *Accounting of Disclosures* Log.
10. The subpoena and any documents produced for the subpoena will be retained according to state and federal regulations.



Policy & Procedure

HIPAA / PRIVACY RESPONDING TO A SUBPOENA

FUNCTION
HIPPA

NUMBER
1004

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

Pinnacle Health Management **RESPONSE TO SUBPOENA NOT ACCOMPANIED BY A COURT ORDER AND LACKING SATISFACTORY ASSURANCES OF NOTICE OR QUALIFIED PROTECTIVE ORDER**

[Date]

[Attorney Name and Address]

Re: [name of resident]

Dear [Attorney]:

The subpoena you caused to be issued dated _____ requesting copies of protected health information for _____ fails to comply with the applicable requirements of the HIPAA privacy regulations, specifically 45 CFR §164.512(e). As a covered entity, we are allowed to release health information only in accordance with these privacy regulations.

Accordingly, we recommend you either secure an authorization in conformity with 45 CFR 164.508 directly from [name of resident or his/her personal representative] for release of the requested protected health information or take the following steps pursuant to 45 CFR section 164.512(e):

- a) Secure a Court Order detailing your specific needs pursuant to 45 CFR § 164.512(e)(1)(i);
or
- b) Provide us with satisfactory assurance as described at 45 CFR 164.512(e)(1)(ii)(A) that you have made reasonable efforts to notify [name of resident] of your request for protected health information. This requires you to provide us with a written statement and accompanying documentation assuring us that you have made a reasonable effort to provide [name of resident] with a written notice of your request. This written statement you provide to us must also attest that the written notice you provided [name of resident] included:
 - 1. Sufficient information about the litigation or proceeding in which the protected health information is requested to permit [name of resident] to raise an objection to the court or administrative tribunal; and that
 - 2. The time for [name of resident] to raise objections to the court or administrative tribunal has elapsed; and

Policy & Procedure



HIPAA / PRIVACY RESPONDING TO A SUBPOENA

FUNCTION

HIPPA

NUMBER

1004

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

3. No objections were filed; or
 4. All objections filed by [name of resident] have been resolved by the court or administrative tribunal and the disclosures or protected health information being sought are consistent with such resolution; or you may
- c) Provide us satisfactory assurance as described at 45 CFR 164.512(e)(1)(iv) that you have made reasonable efforts to secure a qualified protective order that meets the requirements set forth at 45 CFR 164.512(e)(1)(v). The satisfactory assurance you provide us must include a written statement and accompanying documentation demonstrating that:
1. The parties to the dispute giving rise to the request for protected health information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
 2. The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

A "qualified protective order", as the term is used in paragraph (c) above means: an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- a) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
- b) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

We respectfully ask that if you are not able to meet one of the identified exceptions above regarding disclosure of protected health information, thereby allowing us to release such information in a manner compliant with the regulations cited, that you withdraw your subpoena request until such time as one of the requirements can be met.

Sincerely,

[Privacy Official]

Cc: [Director or administrator]

Policy & Procedure



HIPAA / PRIVACY COMPLAINTS

FUNCTION
HIPPA

NUMBER
1005

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

PURPOSE

To ensure that an effective complaint process is in place to deal with privacy violations. The process is to include:

- Identification of a privacy designee who is responsible for receiving complaints.
- A method for documenting receipt of complaints and their resolution.
- Assurance that no individual will be required to waive their rights to file a complaint with the Department of Health and Human Services.

POLICY

It is the policy of this Pinnacle Health Management to ensure the privacy of Protected Health Information (“PHI”) as well as to ensure that such information is used and disclosed in accordance with all applicable laws and regulations. Any concerned individual has the right to file a formal complaint concerning privacy issues without fear of reprisal. Such issues could include, but are not limited to, allegations that:

- PHI that was used/disclosed improperly; or
- Access or amendment rights were wrongfully denied.

PROCEDURE

1. All residents or their personal representatives have the right to complain to Pinnacle Health Management or the Department of Health and Human Services.
2. All concerns may be registered by telephone, mail, or in person.
3. Upon receipt of a complaint about Pinnacle’s privacy policies or its compliance with those policies or the law, the complaint will be recorded on a *Complaint Log* or *Complaint Regarding Use or Disclosure of Protected Health Information (“Complaint”)* form. (See *Complaint* form and *Complaint Log* following this Policy.)
4. Pinnacle Health Management’s Privacy Official will review the *Complaint* form/log to ensure that the information is complete, and take the necessary steps to get complete information:
 - a. Document the date, time, and name of the person making the complaint in the *Complaint Log*.
 - b. Investigate the complaint.
 - c. Document the resolution of the complaint.
5. Once the *Complaint* form/log is completed correctly, Pinnacle Health Management’s Privacy Official will review and investigate the complaint to determine if a violation of the law or Pinnacle’s policies has occurred.

Policy & Procedure



HIPAA / PRIVACY COMPLAINTS

FUNCTION

HIPPA

NUMBER

1005

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

6. The Privacy Official shall determine the substance of the findings and will direct the content and method of response:
 - a. Document the resolution of the complaint.
 - b. Communicate the outcome of the complaint with the individual filing the complaint within 30 days from receipt of complaint.
7. Pinnacle Health Management's Privacy Official shall maintain documentation of all complaints received and their disposition for a period of at least six years (from the date of creation) in accordance with federal regulations.

Pinnacle Health Management
COMPLAINT REGARDING USES/DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Tracking Number _____

This form is to be used to file a complaint with Pinnacle Health Management regarding its privacy policies and procedures, and its compliance with those policies and procedures or the federal Privacy Rule.

When this form is complete, please return it to: 105 Webster Street, Suite 8, Hanover, Ma, 02339

Resident Information	Requester's information (if not the resident)
_____ Name	_____ Name
_____ Location	_____ Relationship to the Customer
_____ Date of Birth	_____ Source of Legal Authority
_____ SSN	_____ Phone Number

Date of incident: _____/or The practice is ongoing

Time of incident: _____/or Not applicable

Please describe the practice or incident about which you wish to complain:

Name & title of person(s) involved, if known: _____

Please describe why you believe that this practice or incident was improper:

Please attach any documentation that supports your complaint to this form.

I certify that the information recorded above is true to the best of my knowledge, and that I have a good faith belief that such practice or incident is a violation of federal laws regarding the handling of a resident's health information or of Pinnacle Health Management's privacy policies and procedures.

Signature:

Date:

This page intentionally left blank.

Pinnacle Health Management
**RESOLUTION OF COMPLAINT REGARDING USES/DISCLOSURES
OF PROTECTED HEALTH INFORMATION**

Person investigating the complaint:

Name _____

Location _____

Tracking Number: _____

Date _____

Resolution or Conclusion of investigation:

Comments:

Date and Time Resolution Communicated to Individual:

Approval of Privacy Officer

Name _____ Date _____

Comments/Instructions:

This page intentionally left blank.

Pinnacle Health Management
LOG OF INTERNAL COMPLAINTS REGARDING PRIVACY ISSUES

DATE RECEIVED	IDENTITY OF INDIVIDUAL MAKING COMPLAINT (IF KNOWN)	PERSON RECEIVING COMPLAINT	NATURE OF COMPLAINT	STEPS TAKEN TO RESOLVE COMPLAINT	DATE OF RESOLUTION	Method Filed	Tracking Number
Example: 04/30/03	Hotline – anonymous	Pam Peters – privacy officer	Computer screens at nursing station not shielded from visitor view	Computer terminals moved to area at nursing station where they cannot be seen by passerby; monitor screen shields installed	05/02/03		



Policy & Procedure

HIPAA / PRIVACY
COMPLAINTS

FUNCTION HIPPA
NUMBER 1004
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

This page intentionally left blank.

Policy & Procedure



HIPAA / PRIVACY DESIGNATED RECORD SET

FUNCTION
HIPAA

NUMBER
1006

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

PURPOSE

To describe the documents that comprises the Designated Record Set.

POLICY

The HIPAA Privacy Rule requires that residents be permitted to request access and amendment to their Protected Health Information ("PHI") that is maintained in a Designated Record Set. This policy documents the contents of the Designated Record Set.

PROCEDURE

1. The Designated Record Set is a group of records maintained by or for the practitioner that consists of the Medical Records maintained at the nursing home or assisted living facility where the resident is seen and Pinnacle Health Management billing records and electronic copies of clinical reports created by each clinician. The term *record* means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the practitioner.
2. Pinnacle Health Management maintains the following as the Designated Record Set:
 - a. The resident's Business Office billing history as entered into the web based billing program known as Psyquel, and
 - b. Copies of clinical reports authored by the clinician; the original report is filed in the resident's medical record at the nursing home or assisted living facility where see.
3. Contributions to the Facility Medical Record on behalf of residents' followed by Pinnacle Health Management, may include the following:
 - Informed consent
 - Physician and professional consultant progress notes

 - Initial diagnostic assessments and evaluations

Policy & Procedure



HIPAA / PRIVACY DESIGNATED RECORD SET

FUNCTION HIPAA
NUMBER 1006
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

- a. If records from other providers are used by the practitioner to make decisions related to the care and treatment of the resident, then these records are considered part of the Facility's Medical Record Designated Record Set, e.g., history and physical, discharge summary and labs from previous acute care hospitalization.
4. The Resident's Business Office Billing File includes, at a minimum, the following:
 - Health plans, including Medicare, Medicaid and other payor sources
 - Resident claim information, including claim, remittance, eligibility response, and claim status response
 - Statements of account balance
 - Collection activity documents and correspondence
5. The Designated Record Set is to be retained according to state and federal regulations and following Facility or company retention procedures.



Policy & Procedure

HIPAA / PRIVACY AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

FUNCTION	HIPAA
NUMBER	1007
PRIOR ISSUE	
EFFECTIVE DATE	10/01/2014

PURPOSE

The purpose of this Policy is to set forth Pinnacle Health Management’s process for the use and disclosure of Protected Health Information (“PHI”) pursuant to a written authorization.

POLICY

In accordance with the HIPAA Privacy Rule, when PHI is to be used or disclosed for purposes other than treatment, payment, or health care operations, Pinnacle Health Management will use and disclose it only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization.

PROCEDURE

Exceptions to Authorization Requirements

PHI may be disclosed without an authorization if the disclosure is:

1. Requested by the resident or his duly authorized representative (authorization is never required);
2. For the purpose of treatment;
3. For the purpose of Pinnacle Health Management’s payment activities, or the payment activities of the entity receiving the PHI;
4. For the purpose of Pinnacle Health Management’s health care operations;
5. In limited circumstances, for the health care operations of another Covered Entity, if the other Covered Entity has or had a relationship with the resident;
6. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the HIPAA Privacy Rule; or
7. Required by other state or federal law. (See “Request and Disclosure Table” in the “Uses and Disclosures of Protected Health Information” Policy for other exceptions.)

Use or Disclosure Pursuant to an Authorization

1. When Pinnacle Health Management receives a request for disclosure of PHI, Pinnacle Health Management’s Privacy Official shall determine whether an authorization is required prior to disclosing the PHI.
2. PHI may never be used or disclosed in the absence of a valid written authorization if the use or disclosure is:
 - a. Of psychotherapy notes as defined by the HIPAA Privacy Rule;
 - b. For the purpose of marketing; or



Policy & Procedure

HIPAA / PRIVACY AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1007

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- c. For the purpose of fundraising.
3. If the use or disclosure requires a written authorization, Pinnacle Health Management shall not use or disclose the PHI unless the request for disclosure is accompanied by a valid authorization.
4. If the request for disclosure is not accompanied by a written authorization, Pinnacle Health Management's Privacy Official shall notify the requestor that it is unable to provide the PHI requested. The Privacy Official will supply the requestor with an *Authorization to Use or Disclose PHI ("Authorization")* form.
(See sample *Authorization* form following this Policy.)
5. If the request for disclosure is accompanied by a written authorization, the Privacy Official will review the authorization to assure that it is valid (see the "Checklist for Valid Authorization" following this Policy).
6. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Privacy Official will notify the requestor, in writing, of the deficiencies in the authorization. No PHI will be disclosed unless and until a valid authorization is received.
7. If the authorization is valid, the Privacy Official will disclose the requested PHI to the requester. Only the PHI specified in the authorization will be disclosed.
8. Each authorization shall be filed in the resident's Medical Record.

Preparing an Authorization for Use or Disclosure

1. When Pinnacle Health Management is using or disclosing PHI and an authorization is required for the use or disclosure, Pinnacle Health Management will not use or disclose the PHI without a valid written authorization from the resident or the resident's personal representative.
2. The *Authorization* form must be fully completed, signed and dated by the resident or the resident's personal representative before the PHI is used or disclosed.
3. Pinnacle Health Management may not condition the provision of treatment on the receipt of an authorization except in the following limited circumstances:
 - a. The provision of research-related treatment; or
 - b. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).
4. An authorization may not be combined with any other document unless one of the following exceptions applies:



Policy & Procedure

HIPAA / PRIVACY AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1007

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- a. Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;
- b. Authorizations to use or disclose psychotherapy notes may only be combined with another authorization related to psychotherapy notes; or
- c. Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if Pinnacle Health Management has not conditioned the provision of treatment or payment upon obtaining the authorization.

Revocation of Authorization

1. The resident may revoke his authorization at any time.
2. The authorization may ONLY be revoked in writing. If the resident or the resident's duly authorized representative informs Pinnacle Health Management that he/she wants to revoke the authorization, Pinnacle Health Management will assist him/her to revoke in writing.
3. Upon receipt of a written revocation, the Privacy Official will write the effective date of the revocation on the *Authorization* form.
4. Upon receipt of a written revocation, Pinnacle Health Management may no longer use or disclose a resident's PHI pursuant to the authorization.
5. Each revocation will be filed in the resident's Medical Record.

This page intentionally left blank.

Pinnacle Health Management
AUTHORIZATION TO USE AND/OR DISCLOSE HEALTH INFORMATION

<p>Revocation</p> <p>Date Revoked: _____</p> <p>Initials of Privacy Official _____</p>

Resident Name: _____ Medical Record No. _____

Address: _____

Facility Name: _____

I authorize this Facility to use or disclose my health information as described below.

1. **Type of information:** The type of information to be used or disclosed is as follows (check the appropriate spaces and include other information where indicated):

<input type="checkbox"/> The entire medical record (all information)	
<input type="checkbox"/> The entire Medical Record (all information)	<input type="checkbox"/> Minimum Data Set
<input type="checkbox"/> Activity documentation	<input type="checkbox"/> Nursing documentation/progress notes
<input type="checkbox"/> Assessments, flow sheets	<input type="checkbox"/> Nutritional services documentation
<input type="checkbox"/> Business Office File	<input type="checkbox"/> Physician and professional consult progress notes
<input type="checkbox"/> Care Plan	<input type="checkbox"/> Physician's orders
<input type="checkbox"/> Diagnostic reports (lab, x-ray, etc.)	<input type="checkbox"/> Rehabilitative and restorative therapy documentation
<input type="checkbox"/> History and physical, other hospital records	<input type="checkbox"/> Social Services documentation
<input type="checkbox"/> Medication and treatment records	
<input type="checkbox"/> Other: (Describe as specifically as possible).	

2. **Recipient of information** - The information identified above may be used by, or disclosed to, the following individual(s) or organization(s):

Name: _____ Name: _____

Address: _____ Address: _____

Name: _____ Name: _____

Address: _____ Address: _____

AUTHORIZATION TO USE AND/OR DISCLOSE HEALTH INFORMATION -page 2

3. **Purpose of use/disclosure** - This information described on the previous page will be used for the following purpose(s):

____ Initiated at the request of the resident.

____ My personal records

____ Sharing with other health care providers as needed

____ Other (please describe): _____

Authorization Statements/Signatures:

4. I understand that once the above information is disclosed, it may be re-disclosed by the recipient and the HIPAA Privacy Rule may no longer protect the information.

5. **For Marketing disclosures only: (Check if applicable)** _____ I understand that Pinnacle Health Management will receive compensation related to the use or disclosure of the requested information.

6. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization, I must do so in writing and present my written revocation to a licensed Facility staff member. I understand that the revocation will not apply to information that has already been released in response to this authorization.

7. Unless I specify differently, this authorization will expire (insert date or event):

8. I understand that Pinnacle Health Management will not condition the provision of treatment or payment on the provision of this authorization.

Signature of Resident or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Distribution of copies: Original to resident's Medical Record, copy to resident.

CHECKLIST FOR VALID AUTHORIZATION

When you receive a request for release of Medical Records containing PHI from any entity other than the resident or the resident's personal representative, and the disclosure is not for purposes of treatment, payment or health care operations or another disclosure required or permitted by the HIPAA Privacy Rule, you may not release those records unless the requestor has provided a valid authorization. Use this checklist to assure that the authorization is valid. **If any one element is missing, the Privacy Rule prohibits you from disclosing the information.** You should contact the requestor and explain why you cannot disclose the information.

_____The authorization must be written in plain language.

All of the following elements must be included in the authorization:

_____A specific and meaningful description of the information to be disclosed.

_____The name or other specific identification of the person (or organization or class of persons) authorized to make the requested disclosure.

_____The name or other specific identification of the person (or organization or class of persons) to whom the information will be disclosed.

_____The purpose of the requested disclosure. (If the resident initiates the authorization, the statement "at the request of the resident" is a sufficient description of the purpose).

_____An expiration date or an expiration event that relates to the resident or the purpose of the disclosure.

_____Signature of the resident or personal representative and date.

_____If signed by personal representative, a description of the representative's authority to act for the resident.

Required Statements:

_____A statement that information disclosed pursuant to the authorization may be subject to redisclosure and may no longer be protected by the Privacy Rule.

_____A statement of the resident's right to revoke the authorization in writing and either,

_____A reference to the revocation right and procedures described in the Notice of Privacy Practices;

OR

_____A statement about the exceptions to the right to revoke and a description of how the resident may revoke.

_____One of the following statements, or a substantially similar statement:

- If the Covered Entity is not permitted to condition treatment or payment on the provision of an authorization: I understand that Pinnacle Health Management will not condition the provision of treatment or payment on the provision of this authorization.

OR

- If the Covered Entity is permitted to condition the provision of research-related treatment on the provision of an authorization: I understand that Pinnacle Health Management will not provide research-related treatment to me unless I provide this authorization.

OR

- If the Covered Entity is permitted to condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization: I understand that Pinnacle Health Management will not provide health care that is solely for the purpose of creating PHI for disclosure to a *third party* to me unless I provide this authorization.

▪

Defective Authorizations

If an authorization has any one of the following defects, it is invalid and any use or disclosure made pursuant to the authorization will be in violation of the Privacy Rule:

_____ The authorization has expired.

_____ One of the required elements or statements is missing.

_____ Pinnacle Health Management has knowledge that the authorization has been revoked.

_____ The authorization violates the regulations governing conditioning treatment or payment upon signing the authorization, or combining authorizations.

_____ Pinnacle Health Management has knowledge that information in the authorization is false.

Policy & Procedure



HIPAA / PRIVACY MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

NUMBER

PRIOR ISSUE

EFFECTIVE DATE

PURPOSE

To ensure Pinnacle Health Management's uses and disclosures of Protected Health Information ("PHI") are limited to the minimum necessary to accomplish the intended purpose.

POLICY

It is the policy of Pinnacle Health Management to make a reasonable effort to use or disclose, or to request from another health care provider, the minimum amount of PHI required to achieve the particular use or disclosure unless an exception applies.

For any non-routine request for disclosure of PHI that does not meet an exception, Pinnacle Health Management will review the request for disclosure on an individual basis.

Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.

PROCEDURE

1. Pinnacle Health Management will identify role based access to PHI per job description, including:
 - a. People or classes of people in its workforce who need access to PHI to carry out their duties, and
 - b. The category or categories of PHI to which access is needed, including any conditions that may be relevant to such access.

(See Sample "Role Based Access to PHI" table following this Policy.)

2. Pinnacle Health Management, for any type of disclosure or request for disclosure that is made on a routine and recurring basis, will limit the disclosed PHI, or the request for disclosure, to that which is reasonably necessary to achieve the purpose of the disclosure or request. (See "Examples of Routine Requests and Disclosures" following this Policy.)
3. Pinnacle Health Management, for disclosures or requests for that are not made on a routine and recurring basis (non-routine disclosures), will review the request to verify that PHI disclosed or requested is the minimum necessary.

All requests for non-routine disclosures or requests that do not meet an exception will be reviewed using standard criteria.

4. Exceptions to minimum necessary requirements: Pinnacle Health Management will release information without concern for the minimum necessary standard as follows:
 - a. Disclosures to or requests by a health care provider for treatment.
 - b. Uses or disclosures made to the individual who is the subject of the PHI.

Policy & Procedure



HIPAA / PRIVACY MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

NUMBER

PRIOR ISSUE

EFFECTIVE DATE

- c. Uses or disclosures made pursuant to an authorization signed by the individual.
- d. Disclosures made to the Secretary of the U.S. Department of Health and Human Services (federal government).
- e. Disclosures that are required by law (such as for Department of Health state surveys, federal surveys, public health reportable events, FDA as related to product quality, safety, effectiveness or recalls etc.).
- f. Uses and disclosures that are required for compliance with the HIPAA Privacy Rule.
5. Pinnacle Health Management may use or disclose an individual's entire Medical Record Data Set only when such use or disclosure is specifically justified as the amount that is reasonably necessary to accomplish the intended purpose or one of the exceptions noted above applies.
6. Requests for entire Medical Record Data Set that are not covered by an exception will be reviewed using standard criteria.
7. Reasonable Reliance: Pinnacle Health Management may rely on a requested disclosure as minimum necessary for the stated purpose(s) when:
 - a. Making disclosures to public officials, if the official represents that the information is the minimum necessary for the stated purpose(s).
 - b. The information is requested by another covered entity (health care provider, clearinghouse or health plan).
 - c. The information is requested by a professional who is a member of Pinnacle Health Management's workforce or is a Business Associate of Pinnacle Health Management for the purpose of providing professional services to Pinnacle Health Management, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).
 - d. The information is requested for research purposes and the person requesting the information has provided documentation or representations to Pinnacle Health Management that meet the HIPAA Privacy Rule. Contact the Privacy Officer to assist in the determination of whether such requirements have been met. (See Policy "Uses and Disclosures of Protected Health Information for Research.")
8. Pinnacle Health Management, upon determination that the use, disclosure or request for PHI is the minimum necessary or one of the above exceptions apply (see Items 4 and 6), will release the PHI to the requestor.
9. Facility Requests for PHI from Another Covered Entity: When requesting PHI from another Covered Entity, Pinnacle Health Management must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are made on a routine and recurring basis, Pinnacle Health Management shall

Policy & Procedure



HIPAA / PRIVACY MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

NUMBER

PRIOR ISSUE

EFFECTIVE DATE

take reasonable steps to insure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

For requests that are not on a routine or recurring basis, Pinnacle Health Management shall evaluate the request according to the following criteria:

- a. Is the purpose for the request stated with specificity?
- b. Is the amount of PHI to be disclosed limited to the intended purpose?
- c. Have the requirements for supporting documentation, statements, or representations been satisfied? (See policy "Uses and Disclosures of Protected Health Information" for specific requirements.)
- d. Have all applicable requirements of the HIPAA Privacy Rule been satisfied with respect to the request?

ROLE BASED ACCESS TO PHI

LEVEL 1: None – No Access to Designated Record Set (i.e. Volunteer)

LEVEL 2: May access minimum necessary PHI (not Designated Record Set) to complete assigned tasks and/or to document actions (i.e. PHI discussed)

LEVEL 3: Full access to the Medical Record subset of the Designated Record Set

LEVEL 4: Full access to the Business Office File subset of the Designated Record Set

Position	Access Level			Explanation/Duties Performed Requiring Access
Business Office Manager	x	x	x	Operations/Payment
Business Office Staff	x		x	Operations/Payment
Nurse Practitioner	x	x	x	Treatment/Operations
Privacy Official	x	x	x	Treatment/Payment/Operations
LICSW	x	x	x	Treatment/Payment/Operations
Psychologists	x	x	x	Treatment/Payment/Operations

EXAMPLES OF ROUTINE REQUESTS AND DISCLOSURES

Requester	Purpose	Disclosures
Ambulance Co.	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
Coroner	Investigate a suspicious death	Specific information requested
Disability Determination	Evaluate individual's medical condition in support of disability benefits	Specific information requested
Insurance Co	Substantiate care provided for payment	Specific information requested in claims attachment request
Healthcare oversight agency	Investigate a complaint	Protected health information related to complaint
Physician or other practitioner	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
State data commission	Support a statewide registry	File of specific data elements requested

Policy & Procedure



HIPAA / PRIVACY FAXING PROTECTED HEALTH INFORMATION

FUNCTION
HIPPA

NUMBER
1009

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

PURPOSE

To ensure that Protected Health Information (“PHI”) is appropriately safeguarded when it is sent or received via facsimile (fax) machine or software.

POLICY

It is the policy of Pinnacle Health Management to allow the use of facsimile machines to transmit and receive PHI. The information released will be limited to the minimum necessary to meet the requestor’s needs.

PROCEDURE

1. The fax machine used to transmit PHI to Pinnacle Health Management should be located in an area that is not easily accessible to unauthorized persons. Examples include the Facility’s business office, medical record office or nurse’s station. If possible, the fax machine should not be located in a public area where confidentiality of PHI might be compromised. If this is not possible, a sign should be posted regarding access to the documents. (See sample sign following this Policy.)
2. Transmission to Pinnacle Health Management is received through a secure portal provided through Intermedia. Each document to be faxed shall contain a cover letter with specific instructions for the documents destruction should delivery to an errant number occur.
3. Unless otherwise prohibited by state law, information transmitted via facsimile is acceptable and may be included in the resident’s Medical Record.
4. Steps should be taken to ensure that the fax transmission is sent to the appropriate destination. These include:
 - a. Asking frequent recipients to notify Pinnacle Health Management of a fax number change.
 - b. Confirming the accuracy of the recipient’s fax number before pressing the send/start key.
 - c. If possible, printing a confirmation of each fax transmission.
5. A cover page should be attached to any facsimile document that includes PHI. (See a sample cover page following this Policy.) The cover page should include:
 - a. Destination of the fax, including name, fax number and phone number;
 - b. Name, fax number and phone number of the sender;
 - c. Date;
 - d. Number of pages transmitted; and



Policy & Procedure

HIPAA / PRIVACY FAXING PROTECTED HEALTH INFORMATION

FUNCTION

HIPPA

NUMBER

1009

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- e. Confidentiality Statement (See sample below).
- 6. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system should be checked to obtain incorrect recipient's fax number. Fax a letter to the receiver and ask that the material be returned or destroyed.
- 7. A written *Authorization* for any use or disclosure of PHI will be obtained when the use or disclosure is not for treatment, payment or healthcare operations or required by federal or state law or regulation.
- 8. The PHI disclosed will be the minimum necessary to meet the requestor's needs.

Sample Confidentiality Statement:

The documents accompanying this transmission contain confidential protected health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

FAX COVER PAGE

Pinnacle Health Management
125 Church St, Suite 90-104
Telephone: 781-754-6545
Fax: 781-536-0016

Confidential and Protected Communication

FAX COVER SHEET

DATE & TIME _____ NUMBER OF PAGES _____

TO: _____
NAME _____

FAX NUMBER _____ PHONE NUMBER _____

FROM: _____

COMMENTS:

VERIFICATION OF RECEIPT OF FAX:

This communication may contain confidential Protected Health Information. This information is intended only for the use of the individual or entity to which it is addressed. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

*If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is STRICTLY PROHIBITED by Federal law. **If you have received this information in error, please notify the sender immediately** and arrange for the return or destruction of these documents*

This page intentionally left blank.

SIGN FOR FAX MACHINE



**Only authorized staff may view
faxed documents sent or received
by this fax machine.**

Access to such documents by unauthorized persons is prohibited by federal law.



Policy & Procedure

HIPAA / PRIVACY
**ACCOUNTING OF DISCLOSURES
OF PROTECTED HEALTH INFORMATION**

FUNCTION HIPAA
NUMBER 1010
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

This page intentionally left blank.



Policy & Procedure

HIPAA / PRIVACY ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1010

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

Residents have the right to receive an accounting of the disclosures of their Protected Health Information (“PHI”). The following is the process for responding to a resident’s request for an accounting of disclosures of their PHI made by Pinnacle Health Management.

POLICY

Each resident may request and receive an accounting of trackable disclosures of PHI made by Pinnacle Health Management. Pinnacle Health Management will provide such an accounting, in accordance with the HIPAA Privacy Rule, when requested by a resident or a resident’s duly authorized representative. The requested information will not include PHI released or disclosed on or prior to April 13, 2003.

Records of disclosures are retained for a six-year period.

PROCEDURE

1. Upon receiving an inquiry from a resident, Pinnacle Health Management’s Privacy Official provides the resident or duly authorized representative with a copy of a *Request for an Accounting of Disclosures of PHI* (“Request”) form. (See sample *Request* form following this Policy.)

Requests are not evaluated until the *Request* form is completed and signed by the resident or personal representative.

2. Pinnacle Health Management’s Privacy Official reviews and processes the request.
3. Pinnacle Health Management provides a written accounting no later than 60 days after receipt. If Pinnacle Health Management is unable to meet the 60-day time frame, Pinnacle Health Management may extend the time once by no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay and the date by which Pinnacle Health Management will provide the accounting. (See the *Notification of Time Extension* form in the Policy “Former Resident’s Access to Protected Health Information.”)
4. A written accounting is provided to the requestor using an *Accounting of Disclosures* log. (See sample log following this Policy.)
 - a. The accounting will include disclosures during the period specified by the resident or personal representative in the request. The specified period may be up to six years prior to the date of the request. Disclosures made on or before April 13, 2003 will not be included in the accounting.
 - b. Pinnacle Health Management will include known disclosures made by its Business Associates, if aware of any such disclosures required to be included in an accounting.



Policy & Procedure

HIPAA / PRIVACY ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION HIPAA
NUMBER 1010
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

- c. For each disclosure, the accounting will include:
 - i. Date the request for disclosure was received;
 - ii. Name of entity requesting disclosure and, if known, the address of such person or entity;
 - iii. A brief description of the PHI that was disclosed; and
 - iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
- d. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, Pinnacle Health Management may provide:
 - i. The first disclosure during the accounting period;
 - ii. The frequency, or number of disclosures made during the accounting period;
 - iii. The date of the last such disclosure during the accounting period.
- 5. For disclosures of PHI for research purposes in a project consisting of fifty or more individuals, the accounting may provide:
 - a. Name of protocol or other research activity;
 - b. Description and purpose of research, criteria for selecting particular records;
 - c. Brief description of the type of PHI disclosed;
 - d. Date or period of time during which disclosure(s) occurred, including date of last disclosure during accounting period;
 - e. Name, address, telephone number of entity that sponsored the research and of the researcher to whom the information was disclosed;
 - f. Statement that PHI of the resident may or may not have been disclosed for a particular protocol or the research activity.
- 6. Pinnacle Health Management will provide the first accounting to a resident or personal representative within a 12-month period without charge. However, Pinnacle Health Management may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided Pinnacle Health Management has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.
- 7. Pinnacle Health Management may exclude those disclosures that qualify as an exception.
- 8. Pinnacle Health Management must document and retain for six years from the date of the accounting:
 - a. The information required to be included in the accounting, and



Policy & Procedure

HIPAA / PRIVACY
**ACCOUNTING OF DISCLOSURES
OF PROTECTED HEALTH INFORMATION**

FUNCTION
HIPAA

NUMBER
1010

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

- b. The written accounting provided to the requesting party.

POTENTIAL AREAS WHERE ACCOUNTING OF DISCLOSURES APPLIES:

1. Disclosures to Public Health Authorities

- For the purpose of preventing or controlling disease, injury or disability
- To conduct public health surveillance
- For public health investigations and interventions
- For reporting vital events such as births and deaths
- To a foreign government agency at the request of a public health authority
- To report child/elder abuse
- If necessary, to prevent or lessen a serious and imminent threat to the health or safety of an resident or the public

2. Disclosures to an Entity Subject to the Food and Drug Administration

- To report adverse events, product defects or biological product deviations
- To track products
- To enable product recalls, repairs or replacements
- To conduct post marketing surveillance

3. Disclosures to an Employer

- Only PHI specific to a work-related illness or injury, and
- Required for the employer to comply with its obligations under federal or state occupational safety and health laws

4. Disclosures to Health Oversight Agencies

- For government benefit program eligibility
- To determine compliance with civil rights laws
- For civil, administrative or criminal investigations, proceedings or actions

5. Disclosures in Judicial and Administrative Proceedings

- In response to a court order or court ordered warrant
- In response to a subpoena, only if approved by Extencicare's Legal Department

6. Disclosures to Law Enforcement Officials

- For the purpose of locating a suspect, fugitive, material witness or missing person
- About a resident who is or is suspected to be a victim of a crime
- Regarding crimes on Pinnacle Health Management premises
- Regarding suspicious deaths



Policy & Procedure

HIPAA / PRIVACY ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1010

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- In response to an administrative request, civil investigative demand or grand jury subpoena, after review by Extendicare's Legal Department
 - For the purpose of averting a serious threat to health or safety
- 7. Disclosures about victims of abuse, neglect or domestic violence**
- To a government authority authorized by law to receive reports of abuse, neglect or domestic violence
- 8. Disclosure of Deceased Persons' PHI**
- To the Coroner, Medical Examiner or Funeral Directors
 - To organ procurement organizations
- 9. Disclosures for research**
- Only if disclosure was made without an authorization as permitted by the Privacy rule
- 10. Disclosures for Specialized Government Functions**
- To Armed Forces personnel for military purposes
 - To authorized federal officials for the protection of the President and other Federal officials
 - To other government agencies, if approved by Extendicare's Legal Department
- 11. Disclosures for Worker's Compensation**
- As authorized by and to the extent necessary to comply with the law

EXCEPTIONS TO ACCOUNTING OF DISCLOSURES:

Accounting of disclosure does not include disclosures:

- Necessary to carry out treatment, payment, and health care operations
- To the resident for whom the PHI was created or obtained
- Pursuant to a signed authorization by the resident or personal representative
- For national security or intelligence purposes
- To a correctional institution
- Temporarily suspended by a law enforcement official or health oversight agency (exception applies only during the period of suspension)
- That are incidental
- As part of a Limited Data Set
- That occurred on or prior to April 13, 2003

Pinnacle Health Management
REQUEST FOR AN ACCOUNTING OF DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Resident's Name: _____ Medical Record Number: _____

Facility's Name: _____ Facility Number: _____

Date Range to be Included

I would like an accounting of disclosures of my Protected Health Information (PHI) for the following time frames.

(Please note the maximum time frame that can be requested is six years prior to the date of this request.)

From Date _____	To Date _____
From Date _____	To Date _____
From Date _____	To Date _____

Fees

First request in a 12-month period:	Free
Subsequent Requests:	(Cost-based fee per entity)

I understand that there may be a fee for this accounting and wish to proceed. I also understand that the accounting will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

Qualified Exceptions to the Accounting

I understand that, by law, Pinnacle Health Management is not required to account for disclosures that meet the following criteria:

- The disclosure was necessary to carry out treatment, payment, and health care operations.
- The disclosure was to the resident for which the PHI was created or obtained.
- The disclosure was pursuant to a signed authorization by the resident or personal representative.
- The disclosure was for Pinnacle Health Management's directory or to persons involved in the resident's care or other notification purposes.
- The disclosure was for national security or intelligence purposes.
- The disclosure was to a correctional institution or law enforcement official.
- The disclosure occurred prior to April 13, 2003.

Signature of Resident or Personal representative

Date

Distribution of copies: Original to resident's Medical Record, copy to resident

This page intentionally left blank.



Policy & Procedure

HIPAA / PRIVACY AMENDMENT OF PROTECTED HEALTH INFORMATION

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

This page intentionally left blank.



Policy & Procedure

HIPAA / PRIVACY AMENDMENT OF PROTECTED HEALTH INFORMATION

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

PURPOSE

This Policy is to provide a process for responding to a resident’s request for an amendment to Protected Health Information (“PHI”).

POLICY

A resident has the right to request that Pinnacle Health Management amend his PHI maintained in the Designated Record Set for as long as the PHI is maintained. The policy of this Facility is to respond to a resident’s request for amendment of PHI in accordance with the HIPAA Privacy Rule. This policy contains the procedures for approving an amendment, denying an amendment and making an amendment at the request of another covered entity.

Note: The *Notice of Privacy Practices* states that an amendment is not necessary to correct clerical errors.

PROCEDURE

1. The resident has the right to amend his PHI at any time.
2. Pinnacle Health Management’s Privacy Official (“Privacy Official”) will process all requests for amendment.
3. Upon receiving an inquiry from a resident regarding the right to amend his/her PHI, the Privacy Official will provide the resident with a copy of an *Amendment of Protected Health Information (“Amendment of PHI”)* form. A request for amendment will not be evaluated until the request form is completed and signed by the resident or personal representative.
(See sample *Amendment of PHI* form following this Policy.)

Evaluating and Responding to the Request for Amendment

1. The Privacy Official will date stamp or write the date received and initial the *Amendment of PHI* form.
2. The Privacy Official will make a determination to accept or deny the amendment after consultation with the appropriate staff, if needed.
3. The Privacy Official shall act on the request for amendment no later than 60 days after receipt of the request.
 - a. If the amendment is accepted, Facility staff shall make the amendment and inform the resident within 60 days of the written request.
 - b. If the amendment is denied, Pinnacle Health Management shall notify the resident in writing of the denial within 60 days of the written request.



Policy & Procedure

HIPAA / PRIVACY AMENDMENT OF PROTECTED HEALTH INFORMATION

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

4. If Pinnacle Health Management is unable to act on the request for amendment within 60 days of receipt of the request, it may have one extension of no more than 30 days. The Privacy Official will notify the resident in writing of the extension, the reason for the extension and the date by which action will be taken. (See the sample *Notification of Time Extension* in the Policy “Former Resident’s Access to Protected Health Information.”)

Denial of Request for Amendment

1. Pinnacle Health Management may deny the request for amendment in whole or in part if:
 - a. The PHI was not created by Pinnacle Health Management (i.e., an Advance Directive). An exception may be granted if the resident provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment and it is apparent that the amendment is warranted. For example, a hospital or clinic, which has given Pinnacle Health Management information on a resident, has since closed its doors and left no means of obtaining its past information or records that were destroyed by fire or flood with no backup copies available.

Note: This should rarely be the case. Every other avenue will be explored before an amendment is made to information that was not created by Pinnacle Health Management.
 - b. The PHI is not part of the Designated Record Set (i.e., information gathered on worksheets or daily communication sheets that do not become a part of the Medical Record and are not retained).
 - c. The PHI would not be available for inspection under the HIPAA Privacy Rule.
 - d. The PHI that is subject to the request is accurate and complete.
2. If the Privacy Official, in consultation with the appropriate staff, determines that the request for amendment is denied in whole or in part, the Privacy Official will provide the resident with a timely amendment denial letter. The denial shall be written in plain language and shall contain:
 - a. The basis for the denial;
 - b. A statement that the resident has a right to submit a written statement disagreeing with the denial and an explanation of how the resident may file such statement;
 - c. A statement that, if the resident does not submit a statement of disagreement, the resident may request that Pinnacle Health Management include the resident’s request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment;



Policy & Procedure

HIPAA / PRIVACY AMENDMENT OF PROTECTED HEALTH INFORMATION

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

- d. A description of how the resident may file a complaint with Pinnacle Health Management or to the Secretary of the U.S. Department of Health and Human Services. The description must include the name or title and telephone number of the contact person for complaints. (See the Policy “Complaints.”)
- 3. The resident may submit a written statement of disagreement.
- 4. If the resident submits a written statement of disagreement, Pinnacle Health Management may prepare a written rebuttal to the statement. Pinnacle Health Management shall provide a copy of the written rebuttal to the resident who submitted the statement.
- 5. The following documentation must be appended (or otherwise linked) to the PHI that is the subject of the disputed amendment:
 - a. The resident’s *Amendment of PHI* form;
 - b. Pinnacle Health Management’s amendment denial letter;
 - c. The resident’s statement of disagreement, if any; and
 - d. Pinnacle Health Management’s written rebuttal, if any.

Future Disclosures of PHI that is the Subject of the Disputed Amendment

- 1. If the resident submitted a statement of disagreement, Pinnacle Health Management will disclose all information listed in Item 5. above or an accurate summary of such information with all future disclosures of the PHI to which the disagreement relates.
- 2. If the resident did not submit a statement of disagreement, and if the resident has requested that Pinnacle Health Management provide the *Amendment of PHI* form and the amendment denial letter with any future disclosures, Pinnacle Health Management shall include these documents (or an accurate summary of that information) with all future disclosures of the PHI to which the disagreement relates.

Acceptance of the Request for Amendment

If Pinnacle Health Management accepts the requested amendment, in whole or in part, Pinnacle Health Management will take the following steps:

- 1. Pinnacle Health Management’s Privacy Official shall place a copy of the amendment in the resident’s Medical Record or provide a reference to the location of the amendment within the body of the Medical Record.
- 2. The Privacy Official shall notify the relevant persons with whom the amendment needs to be shared, as identified by the resident on the original *Amendment of PHI* form.



Policy & Procedure

HIPAA / PRIVACY AMENDMENT OF PROTECTED HEALTH INFORMATION

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

3. The Privacy Official shall identify other persons, including Business Associates, that it knows have the PHI and that may have relied on, or could foreseeably rely on, such information to the detriment of the resident. The Privacy Official will inform the resident of, and obtain the resident's agreement to notify such other persons or organizations of the amendment.
4. The Privacy Official shall make reasonable efforts to inform and provide the amendment within a reasonable time to:
 - a. Persons identified by the resident as having received the PHI and needing the amendment;
 - b. Persons, including Business Associates, that Pinnacle Health Management knows have the PHI and may have relied, or could foreseeably rely, on such information to the detriment of the resident.
5. If no additional persons needing notification of the amendment are identified, the Privacy Official shall inform the resident in writing that the amendment has been accepted.

Actions on Notices of Amendment

If another Covered Entity notifies Pinnacle Health Management of an amendment to PHI it maintains, the Privacy Official shall make the amendment to the resident's Designated Record Set.

1. Amendments to the Designated Record Set shall be filed with that portion of the PHI to be amended.
2. Amendments that cannot be physically placed near the original PHI will be filed in an appropriate location.
3. If it is not possible to file the amendment(s) with that portion of the PHI to be amended, a reference to the amendment and its location will be added near the original information location.
4. If the actual amendment is not in an easily recognized location near the original information, the reference should indicate where it could be found.
5. General information regarding requests for amendment, forms relating to amendments and correspondence relating to denial or acceptance of requests to amend will be filed in the resident's Medical Record.

(See sample Acceptance, Denial, and Notification letters following this Policy.)

Pinnacle Health Management
AMENDMENT OF PROTECTED HEALTH INFORMATION

Date Received: _____
Initials of Privacy Official: _____

SECTION A: Resident to complete the following information

Date: _____

Resident Name: _____ Medical Record Number _____

Address: _____

REQUEST:

I hereby request that Pinnacle Health Management amend the following in my Designated Record Set **(check all that apply)**:

My Medical Records My Business Office Files

Date(s) of information to be amended (i.e., date of visit, treatment, or other health care services)

The information is incorrect or incomplete in the following manner:

I request this amendment for the following reason(s):

The information should be amended as follows:

I understand that Pinnacle Health Management may or may not supplement my record with an addendum based on my request. I also understand that Pinnacle Health Management is not able to alter the original documentation in a record under any circumstances. Regardless whether my request is granted or denied, I understand that this request will be made a part of my permanent Medical Record and will be sent as part of the Medical Record in response to any authorized requests for release of my Protected Health Information.

Signature of Resident or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Pinnacle Health Management
AMENDMENT ACCEPTANCE LETTER

[DATE]

[RESIDENT NAME]
[ADDRESS]

Dear [RESIDENT]:

Your request to amend your Protected Health Information (see attached form) has been approved. We will notify the individuals and/or organizations that you identified in the original amendment request.

Very truly yours,

[AUTHOR SIGNATURE]
[PRINTED NAME AND TITLE]

Pinnacle Health Management
AMENDMENT ACCEPTANCE WITH CONSENT TO NOTIFY LETTER

[DATE]

[RESIDENT NAME]
[ADDRESS]

Dear [RESIDENT]:

Your request to amend your Protected Health Information (see attached form) has been approved. We will notify the individuals and/or organizations that you identified in the original amendment request.

In addition, we have identified the following individuals and/or organizations that received your Protected Health Information. We are not permitted to notify these individuals and/or organizations without your written agreement. If you would like us to notify the individuals and/or organizations listed below, you must sign, date, and return this statement to us.

Very truly yours,

[AUTHOR SIGNATURE]
[PRINTED NAME AND TITLE]

I hereby request and consent to the notification of the above-identified persons and/or organizations who have previously received my Protected Health Information regarding the approval of my request for amendment.

Signature of Resident or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Pinnacle Health Management
NOTIFICATION OF AMENDMENT LETTER

[DATE]

[Name of Individual/Organization to Receive *Notification of Amendment*
[ADDRESS]

Re: [RESIDENT]
Approval of *Amendment of Protected Health Information*

Dear [RECIPIENT]

We have agreed to a request from the above-referenced resident to amend his/her Protected Health Information as outlined on the attached form entitled "*Amendment of Protected Health Information.*"

In compliance with the HIPAA Privacy Rule (45 CFR §164.526—Amendment of Protected Health Information), we are providing you with proper notification of this approved amendment.

Thank you.

Very truly yours,

[AUTHOR SIGNATURE]

[PRINTED NAME AND TITLE]



Policy & Procedure

HIPAA / PRIVACY RESTRICTIONS TO PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION	HIPAA
NUMBER	1013
PRIOR ISSUE	
EFFECTIVE DATE	10/01/2014

Pinnacle Health Management AMENDMENT DENIAL LETTER

[DATE]

[RESIDENT NAME]
[ADDRESS]

Dear [RESIDENT]:

Your request to amend your Protected Health Information (see attached form) has been denied for the following reason(s):

You have the right to submit a written statement disagreeing with the denial. If you choose to do so, submit your statement to Pinnacle Health Management’s Privacy Official.

If you do not submit a statement of disagreement, you may request that Pinnacle Health Management include your request for amendment and the denial in any future disclosures of your Protected Health Information.

You may file a complaint with our Facility by contacting Pinnacle Health Management’s Privacy Official at 781-754-6545. You also may file a complaint with the Secretary of the U.S. Department of Health and Human Services. Please contact Pinnacle Health Management’s Privacy Official for contact information.

Very truly yours,

[SIGNATURE]
[PRINTED NAME AND TITLE]



Policy & Procedure

HIPAA / PRIVACY RESTRICTIONS TO PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1013

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To provide a process for a resident to request a restriction to an otherwise permitted use or disclosure of the resident's Protected Health Information ("PHI"), and for Pinnacle Health Management to respond to such request.

POLICY

A resident has the right to request that otherwise permitted uses and disclosures of PHI be restricted. Specifically, the resident may request restrictions on:

- The use and disclosure of PHI for treatment, payment or health care operations, or
- The disclosures to family, friends or others for involvement in care and notification purposes.

Pinnacle Health Management is not required to comply with such requests for restriction, but will consider and may agree to a restriction. Pinnacle Health Management will consider the need for access to PHI for treatment purposes when considering a request for a restriction. A request for restriction must be made in writing. Pinnacle Health Management Privacy Official ("Privacy Official") will notify the resident of its determination with respect to the request.

PROCEDURE

1. The resident will be notified of the right to request restrictions on the use and disclosure of PHI in Pinnacle Health Management's *Notice of Privacy Practices* and that the request must be in writing.
2. The Privacy Official shall manage requests for restrictions. All documentation associated with this request will be placed in the resident's Medical Record.
3. The Privacy Official will provide the resident a *Request to Restrict Use and Disclosure of Protected Health Information* ("*Request to Restrict*") form if the resident asks to make a restriction.

(See *Request to Restrict* form following this Policy.)

4. A request for restriction will not be reviewed until the *Request to Restrict* form is completed and signed by the resident. The Privacy Official may assist the resident in completing the form, if necessary.
5. The Privacy Official will review the request in consultation with other Facility staff to determine the feasibility of the request. Pinnacle Health Management shall give primary consideration to the need for access to the PHI for treatment and payment purposes in making its determination.
6. The Privacy Official shall complete the "Facility Response" section of the *Request to Restrict* form and provide a copy to the resident.



Policy & Procedure

HIPAA / PRIVACY RESTRICTIONS TO PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION
HIPAA

NUMBER
1013

PRIOR ISSUE

EFFECTIVE DATE
10/01/2014

Restriction Not Accepted

If Pinnacle Health Management declines the request for restriction, the Privacy Official will provide the resident with a copy of the signed response (part of the *Request to Restrict* form).

Restriction Accepted

1. If Pinnacle Health Management agrees to the requested restriction, it must abide by the accepted restriction with the following exceptions:
 - a. Pinnacle Health Management may use the restricted PHI, or may disclose such information to a health care provider if:
 - i. The resident is in need of emergency treatment, and
 - ii. The restricted PHI is needed to provide emergency treatment. In this case, Pinnacle Health Management will release the information, but ask the emergency treatment provider not to further use or disclose the resident's PHI.
 - b. Pinnacle Health Management may disclose the information to the individual who requested the restriction.
 - c. Pinnacle Health Management may use and disclose Directory Information unless the resident has objected to such use or disclosure (see the Policy "Uses and Disclosures of Protected Health Information for the Directory").
 - d. Pinnacle Health Management may use and disclose the restricted PHI when statutorily required to use and disclose the information under the HIPAA Privacy Rule.
2. The Privacy Official will notify appropriate Facility staff of the restriction.
3. The Privacy Official will document the restriction on the *Request to Restrict* form, provide the resident with a copy and maintain the original in the resident's Medical Record.

Terminating the Restriction

Termination with the resident's agreement

1. Pinnacle Health Management may terminate the accepted restriction if:
 - a. The resident agrees to the termination in writing; or
 - b. The resident agrees to the termination verbally and the verbal agreement is documented.
2. The Privacy Official will notify the appropriate Facility staff of the termination of the restriction.



Policy & Procedure

HIPAA / PRIVACY RESTRICTIONS TO PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1013

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

3. The Privacy Official will document the resident's agreement to the termination of the restriction on the *Request to Restrict* form, provide the resident with a copy and maintain the documentation in the resident's record.
4. Termination of a restriction with the resident's agreement is effective for all PHI created or received by Pinnacle Health Management.

Termination without the resident's agreement

1. Pinnacle Health Management may terminate the restriction without the resident's agreement if it informs the resident that the restriction is being terminated.
2. Such termination is only effective with respect to PHI created or received after Pinnacle Health Management has informed the resident that it is terminating the restriction.

Note: Pinnacle Health Management must continue to abide by the restriction with respect to any PHI created or received before it informed the resident of the termination of the restriction.

3. Inform by mail: If the resident is informed by mail that Pinnacle Health Management is terminating the restriction, the notification shall be sent via certified mail, return receipt requested. Pinnacle Health Management shall maintain a copy of the notification and of the return receipt with the *Request to Restrict* form. Pinnacle Health Management shall not terminate the restriction until it receives confirmation that the resident has received the notification.
4. Inform in person: It is preferable to have the resident sign and date a notification of termination of a restriction. However, it will be acceptable to document that the resident was so notified on the *Request to Restrict* form.
5. Inform via telephone: If the resident is informed by telephone, this action shall be documented on the *Request to Restrict* form. In addition, a letter shall be sent via certified mail, return receipt requested. The termination shall be effective as of the date the resident is informed by telephone.



Policy & Procedure

HIPAA / PRIVACY
**RESTRICTIONS TO
PERMITTED USES AND DISCLOSURES
OF PROTECTED HEALTH INFORMATION**

FUNCTION HIPAA
NUMBER 1013
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

This page intentionally left blank.

Pinnacle Health Management
REQUEST TO RESTRICT USE AND DISCLOSURE
OF PROTECTED HEALTH INFORMATION

Resident Name: _____ Medical Record No: _____

Address: _____

Facility Name: _____

Directory Information Restriction: I request that the disclosure of my information maintained in Pinnacle Health Management directory be restricted in the following manner:

_____ Do not include my name, location, general condition or religious affiliation in Pinnacle Health Management directory.

_____ Do not disclose my name or religious affiliation to members of the clergy.

_____ Do not disclose my location in the building to: _____.

_____ Do not disclose my general condition to: _____.

Signature of Resident or Personal Representative _____ Date _____

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Other Restrictions: I request the following restriction(s) on the use or disclosure of my Protected Health Information:

_____ Do not release information to the following person(s):

Other restriction (please specify):

Signature of Resident or Personal Representative _____ Date _____

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

**REQUEST TO RESTRICT USE AND DISCLOSURE
OF PROTECTED HEALTH INFORMATION - side 2**

PINNACLE HEALTH MANAGEMENT RESPONSE:

_____ Your request for restriction has been declined.

Note: Pinnacle Health Management may not deny a request for restriction of Directory Information.

_____ Your request for restriction has been accepted. In the case of an emergency or if necessary to comply with the law, we may use and disclose your health information in violation of the restriction. Other than in those circumstances, we will abide by your request unless and until the restriction is terminated (with or without your agreement) and you are notified.

Signature of Pinnacle Health Management Privacy Official

Date

Print Name

TERMINATION OF RESTRICTION

_____ The above name resident agreed to terminate this restriction on: _____.

_____ The above named resident was notified on _____ (date) that this restriction was terminated.

- Resident was notified: (check appropriate box)

_____ In person

_____ By telephone (attach documentation of notification)

_____ By mail (attach documentation of notification)

Signature of Pinnacle Health Management Privacy Official

Date

Print Name

Distribution of copies: Original to resident's Medical Record; copy to resident.



Policy & Procedure

HIPAA / PRIVACY VERIFICATION OF IDENTITY AND AUTHORITY OF OFFICIALS REQUESTING PHI

FUNCTION

HIPAA

NUMBER

1013

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To ensure that Protected Health Information (PHI) is disclosed only to appropriate persons in accordance with the requirements of the HIPAA Privacy Rule.

POLICY

It is the policy of Pinnacle Health Management to verify the identity and the authority of a person making a request for the disclosure of PHI, if the identity or authority of such person is not known to Pinnacle Health Management. Further, Pinnacle Health Management will obtain from the person seeking disclosure of PHI such documentation, statement or representation, as may be required by the HIPAA Privacy Rule, prior to a disclosure.

PROCEDURE

1. In general, Pinnacle Health Management may rely on required documentation, statements or representations that, on their face, meet the verification requirements, if the reliance is reasonable under the circumstances. If there are concerns as to the requirements, contact the legal counsel.
2. Administrative Requests, Subpoena and Investigative Demand: Verification is sufficient and Pinnacle Health Management will disclose the requested PHI if the administrative document itself or a separate written statement recites:
 - a. The information sought is relevant to a lawful inquiry.
 - b. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry.
 - c. De-identified information could not be used.
3. Research: If disclosure is sought for research purposes, pursuant to a waiver of authorization, it is sufficient verification if the requesting documents:
 - a. Show that the waiver of authorization has been approved by a properly constituted Institutional Review Board or Privacy Board.
 - b. Is signed by the Chair of the Board or the Chair's Designee.
4. Requests by a Public Official
 - a. It is sufficient verification of the *identity* of the requesting person to rely on any of the following, if reasonable under the circumstances:
 - i. A badge or other credential
 - ii. A request on government letterhead.

- iii. If the person making the request is acting on behalf of a public official, a written statement on government letterhead that the person is acting on behalf of a public official. If other authority is presented, contact legal counsel for guidance before disclosure.
- b. It is sufficient verification of the *authority* of the requesting person to rely on any of the following, if reasonable under the circumstances:
 - i. A written statement of the authority under which the information is requested, for example, a copy of the law or regulation. Rarely, a written statement is impractical, and then an oral statement is sufficient.
 - ii. Verification of authority is presumed if the request is made pursuant to a warrant, subpoena, order or other process issued by a grand jury, court or judge or administrative tribunal.
- 5. If the disclosure is sought by persons involved in the resident's care, and it is relevant to the requesting party's involvement in the care, practitioners may rely on reasonable professional judgment in verifying the identity and authority of the person seeking disclosure.
- 6. Verification requirements are met if Pinnacle Health Management, in good faith, makes a disclosure of PHI:
 - a. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or
 - b. To law enforcement authorities to identify or apprehend an individual.



Policy & Procedure

HIPAA / PRIVACY DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1014

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To convert individually identifiable Protected Health Information (“PHI”) into information that no longer reveals the identity of any resident.

POLICY

When resident PHI is used or disclosed for purposes other than treatment, payment or health care operations and/or without resident or personal representative authorization, the PHI must be converted into a format that does not identify the resident. This conversion process is called de-identification of PHI.

The Health Insurance Portability and Accountability (HIPAA) Privacy Rule does not apply to de-identified health information.

Pinnacle Health Management meets the de-identification standard if it has removed all of the required identifiers and if Pinnacle Health Management has no actual knowledge that the information could be used to identify a resident.

PROCEDURE

1. Pinnacle Health Management will convert resident PHI into a format that does not identify the resident (de-identify) when:
 - a. PHI is used or shared for purposes other than treatment, payment or health care operations, or
 - b. Information is used or shared without resident authorization.
2. Pinnacle Health Management will de-identify the PHI by one of the following methods:
 - a. Elimination of all identifiers:
 - i. Names.
 - ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code if the geographic area contains more than 20,000 people. If less than 20,000 people are found to be in this area based on the first three digits of the zip code, the code must be changed to 000.
 - iii. All elements of dates (except year) for date directly related to a resident including birth date, admission date, discharge date, date of death: and all ages over 90 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
 - iv. Telephone numbers.

- v. Fax numbers.
- vi. Electronic mail address.
- vii. Social security numbers.
- viii. Medical Record numbers.
- ix. Health plan beneficiary numbers.
- x. Account numbers.
- xi. Certificate/license numbers.
- xii. Vehicle identifiers and serial numbers, including license plate numbers.
- xiii. Device identifiers and serial numbers.
- xiv. Web Universal Resource Locators (URLs).
- xv. Internet Protocol (IP) address numbers.
- xvi. Biometric identifiers, including finger and voiceprints.
- xvii. Full face photographic images and any comparable images.
- xviii. Any other unique identifying number, characteristic, or code.

Note: In addition to removing the above identifiers, Pinnacle Health Management must not have actual knowledge that the information could be used alone or in combination with other information to identify a resident who is a subject of the information.

- b. Statistical De-Identification: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies such principles and determines that the risk is very small that the information could be used to identify the resident. The methods and the results of the analysis must be documented.
3. Re-Identification: Pinnacle Health Management may assign a code that would allow the information to be re-identified by Pinnacle Health Management as long as the code is not derived from or related to information about the resident and is not otherwise capable of being translated so as to identify the resident. Pinnacle Health Management must not use or disclose the code or any other means of record identification for any other purpose and must not disclose the mechanism for re-identification.

Policy & Procedure



HIPAA / PRIVACY BUSINESS ASSOCIATES

FUNCTION

HIPAA

NUMBER

1015

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

The purpose of this Policy is to provide a process for establishing a written agreement with each of Pinnacle Health Management's Business Associates ("BA") as required by the HIPAA Privacy Rule.

POLICY

Pinnacle Health Management contracts with various outside entities and organizations to perform functions or provide services on behalf of Pinnacle Health Management that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are Pinnacle Health Management's Business Associates. The policy of Pinnacle Health Management is to obtain written assurances from BAs that they will appropriately safeguard any PHI they create or receive on Pinnacle Health Management's behalf. Such written assurances will be in place before Pinnacle Health Management discloses PHI to the Business Associate.

PROCEDURE

1. Pinnacle Health Management Administrator will follow established procedures regarding contract review, revision and approval to assure that contract is in compliance with state and federal law.
2. For each contract, determine whether a Business Associate Agreement is necessary. (See the "Business Associate Decision Tree" following this Policy.) Common examples of BAs are:
 - a. A psychologist working on behalf of, but not employed by Pinnacle Health Management or the Facility
 - b. Medical Records Consultant

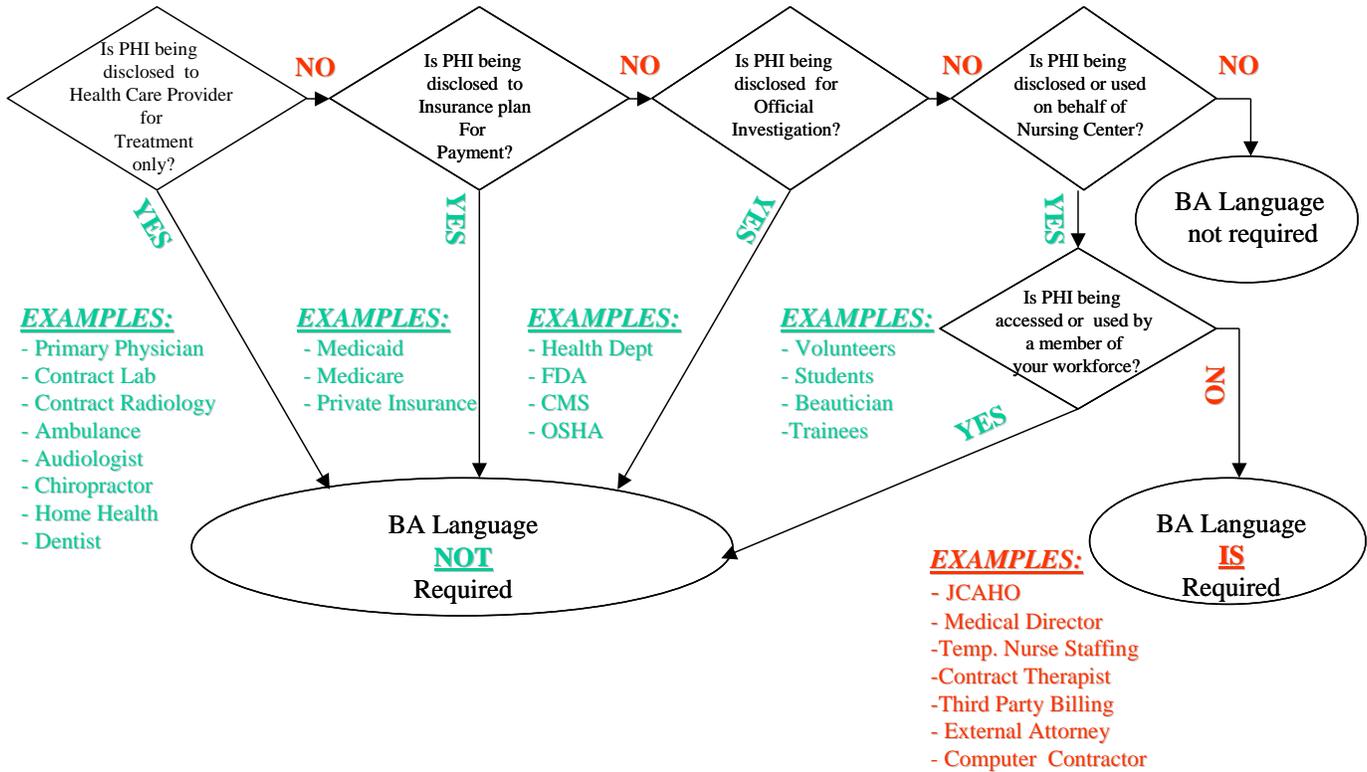
Note: Business Associate language is **not** required when the BA is a health care provider and all disclosures to the BA concern the treatment of a resident.

3. If a BA Agreement is necessary and the third party provides its own BA Agreement, review the Agreement to assure it meets all requirements of the Privacy Rule. (See "Business Associate Checklist" following this Policy.)
4. If a BA Agreement is necessary, and the third party does not provide the Agreement, submit Company's template BA Agreement for approval by the third party.
5. If the BA refuses to sign the BA Agreement, the HIPAA Privacy Rule prohibits Pinnacle Health Management from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of Pinnacle Health Management, Pinnacle Health Management shall not contract with the BA.

6. The original signed contract and contract addendum containing BA language shall be maintained by Pinnacle Health Management.
7. Violations of BA Requirements - If Pinnacle Health Management staff learns of a breach or violation of a BA requirement by a BA, such breach or violation shall be reported to the Privacy Officer, his designee, or to the Compliance Department. The Privacy Officer or Compliance Designee will assist Pinnacle Health Management in determining whether reasonable steps can be taken to cure the breach. If Pinnacle Health Management's reasonable steps to cure the BA's violations are unsuccessful, Pinnacle Health Management may:
 - a. Terminate the contract or arrangement; or
 - b. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.
8. Notice of Termination of a Contract with a BA - Pinnacle Health Management shall notify the Privacy Officer, his designee or the Legal Department when issuing or receiving a notice of contract termination involving a BA. The Legal Department will assist with contacting the BA regarding the BA's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the BA requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

The contract and contract addendum must be retained for six years after the contract was last in effect.

DECISION TREE: WHEN IS BA LANGUAGE REQUIRED?



This page intentionally left blank.

**SAMPLE
BUSINESS ASSOCIATE CHECKLIST**

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
	164.504(e)(2)(i)	Establish permitted and required uses and disclosures of PHI by BA	Final rule – must generally state purposes, reasons for use/disclosure and types of persons to whom info can be disclosed
	164.504(e)(2)(i)	May <u>not</u> authorize BA to use or further disclose info in a manner that would violate requirements of subpart if done by CE except: 	Must include “minimum necessary” language, either within this clause, or as a separate clause. <i>BA shall use/disclose PHI only in the minimum amount and to the minimum number of individuals necessary to achieve the purpose of the services being rendered to or on behalf of CE.</i>
	164.504(e)(2)(i)(A)	May permit BA to use or disclose PHI for “proper management & administration of BA as permitted by (e)(4)	
	164.504(e)(4)(i)(A) and (B)	<u>May permit BA to use PHI</u> – in its capacity as a BA if necessary for the proper management & administration of BA or to carry out the legal responsibilities of BA.	
	164.504(e)(4)(ii)	<u>May permit BA to disclose PHI</u> – in its capacity as a BA for same purposes, but only if disclosure is 	
	164.504(e)(4)(ii)(A)	Required by law or 	
	164.504(e)(4)(ii)(B)(1)	BA obtains reasonable assurances from person to whom info is disclosed that info will be held confidentially and used or further disclosed only as required by law or for purpose for which it was disclosed to the person AND 	
	164.504(e)(4)(ii)(B)(2)	The person to whom the information was disclosed notifies BA of any instance of which it is aware in which the confidentiality of the information has been breached.	
	164.504(e)(2)(i)(B)	BA may provide data aggregation services relating to the health care operations of the covered entity.	

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
	164.504(e)(2)(ii)(A)	BA will not use or further disclose the information other than as permitted or required by the contract or as required by law.	
	164.504(e)(2)(ii)(B)	BA will use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.	
	164.504(e)(2)(ii)(C)	BA will report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware.	Negotiate time and manner of reporting with BA – in writing, to whom, time frame, etc.
	164.504(e)(2)(ii)(D)	BA will ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information.	May want BA to list subcontractors and agents in exhibit.
	164.504(e)(2)(ii)(E)	<u>Access</u> : BA will make available PHI in accordance with 164.524 .	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)(F)	<u>Amendment</u> : BA will make available PHI for amendment and incorporate any amendments to PHI in accordance with 164.526 .	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)(G)	<u>Accounting</u> : BA will document disclosures of PHI as would be required for CE to respond to a request for an accounting.	
	164.504(e)(2)(ii)(G)	<u>Accounting</u> : BA will make available PHI to provide an accounting of disclosures in accordance with 164.528 .	
	164.504(e)(2)(ii)(H)	BA will make internal practices, etc. available to the Secretary.	
	164.504(e)(2)(ii)(I)	<u>Termination</u> : BA will – if feasible – return or destroy all PHI received from, or created or received by the BA on behalf of the CE. BA will retain no copies of such information. If return or destruction of such information is not feasible, BA will extend the protections of the K to the information and limit further uses and disclosures to those purposes that make the return or the destruction of the information infeasible.	
	164.504(e)(2)(iii)	Authorize termination by CE if CE determines that the BA has violated a material term of the contract.	
	Not required by Privacy Rule	<u>MITIGATION</u>	Not required by law, but included in sample language in August final rule.

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
	Not required by Privacy Rule	<u>INSURANCE</u>	If main contract has insurance clause, may not be necessary in addendum.
	Not required by Privacy Rule	<u>Inspection</u> Allow CE to inspect BA's systems, books, records if CE becomes aware of a breach	CE is not required to monitor BA's activities for Privacy Rule purposes.
	Not required by Privacy Rule	<u>INDEMNIFICATION</u>	If main contract has indemnification clause, may not be necessary in addendum.
	Not required by Privacy Rule	<u>Interpretation/ambiguity</u> – broadly as necessary to implement and comply with the Privacy Rule and applicable state laws. Any ambiguity shall be resolved in favor of a meaning that complies and is consistent with the Privacy Rule.	
	Not required by Privacy Rule	<u>Amendment to comply with law</u> - Modification of K to be in compliance with Privacy Rule	
	Not required by Privacy Rule	<u>Assistance in litigation or administrative proceedings</u>	If main contract has this type of clause, may not be necessary in addendum.
	Not required by Privacy Rule	<u>Conflict with contract</u> – addendum controls as it relates to PHI	

This page intentionally left blank.

Policy & Procedure



HIPAA / PRIVACY SANCTIONS

FUNCTION

NUMBER

PRIOR ISSUE

EFFECTIVE DATE

PURPOSE

To ensure there are appropriate sanctions that will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or Pinnacle Health Management's HIPAA privacy policies and procedures.

POLICY

It is the policy of this Facility to discipline employees who fail to comply with Pinnacle Health Management's policies and procedures regarding HIPAA.

PROCEDURE

1. When a concern arises regarding a possible violation of HIPAA or Pinnacle Health Management's policies or procedures related to HIPAA, Pinnacle Health Management's Privacy Official shall begin an investigation promptly. (See the Policy "Complaints" regarding conducting an investigation.)
2. If, at the conclusion of the investigation, it is found that a violation of Pinnacle Health Management's policy or procedure has occurred, the employee involved shall be disciplined in accordance with the severity of the violation and Pinnacle Health Management's disciplinary policy. Violations can be classified according to intent such as:
 - a. Level I Violations are those made accidentally or due to a lack of education.
 - b. Level II Violations are serious violations that are found to show purposeful disregard of Pinnacle Health Management policy.
3. Pinnacle Health Management's Privacy Official shall review the circumstances surrounding any substantiated violation and take appropriate action to mitigate, to the extent possible, any harmful effects of the violation.
4. Documentation from the investigation shall be given to Pinnacle Health Management's Privacy Official to be maintained as a part of Pinnacle Health Management's HIPAA documentation and retained for six years.
5. The disciplinary action report documenting the employee's violation shall be placed in the employee's personnel file as well as a copy provided to Pinnacle Health Management's Privacy Official.



Policy & Procedure

HIPAA / PRIVACY
SANCTIONS

FUNCTION
NUMBER
PRIOR ISSUE
EFFECTIVE DATE

This page intentionally left blank.



Policy & Procedure

HIPAA / PRIVACY RETENTION OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1017

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To ensure appropriate retention of Protected Health Information (“PHI”) contained in a Designated Record Set.

POLICY

PHI contained in the Designated Record Set will be retained according to state and federal regulations whichever requires retention for the longer period of time.

PHI, including medical and financial records contained in the Designated Record Set, will be retained for a minimum of six years as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

In absence of state law specifying a greater retention period, Medical Records must be retained for at least six years after the date it was last in effect.

For minor residents (persons who have not reached full legal age), the Medical Record must be retained for three years after the minor reaches legal age under state law or six years from the date of discharge, whichever is longer.

Medical records on which there may be pending litigation may be exempt from scheduled destruction at the discretion of Pinnacle Health Management.

If state laws and regulations require a greater retention time period, the greater will be followed.

PROCEDURE

1. Pinnacle Health Management will review state laws and regulations to determine Medical Record retention period and “legal age.”
2. If state laws or regulations require a different retention period, the greater retention period will be followed.
3. Pinnacle Health Management will store the records until the retention period has expired. Records must be stored in a secure manner. The records must be protected from unauthorized access and accidental/wrong destruction.
4. At the expiration of the retention period, the Medical Records will be destroyed. Records should be destroyed annually in accordance with the retention time frames.



Policy & Procedure

HIPAA / PRIVACY RETENTION OF PROTECTED HEALTH INFORMATION

FUNCTION HIPAA
NUMBER 1017
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

This page intentionally left blank.



Policy & Procedure

HIPAA / PRIVACY DESTRUCTION OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1018

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

PURPOSE

To ensure that any medium containing Protected Health Information (“PHI”) is properly destroyed.

POLICY

PHI stored in paper, electronic or other format will be destroyed utilizing an acceptable method of destruction after the appropriate retention period has been met.

Access to PHI stored on computer equipment and media will be limited by taking the appropriate measures to destroy electronically stored PHI.

PROCEDURE

Paper Documents:

1. PHI received by the billing office in paper format will be destroyed weekly or sooner as the PHI is a copy and the original document which is filed in the resident’s Facility based Medical Record. (See the Policy “Retention of Protected Health Information.”)
2. All paper documents that contain PHI will be destroyed using an acceptable method of destruction.
3. Acceptable methods of destruction include shredding, incineration, pulverization and use of a bonded recycling company.
4. Prior to destruction of boxed items, Pinnacle Health Management will verify the retention period has expired.
5. If the records are destroyed off-site through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.
6. Pinnacle Health Management will maintain destruction documents permanently.

Computer Data Storage Media

1. Personal Computers: Workstations, laptops and servers use hard drives to store a wide variety of information. Residents’ health information may be stored in a number of areas on a computer hard drive. For example, health information may be stored in “Folders” specifically designated for storage of this type of information, in temporary storage areas and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data.
 - a. To ensure that any residents’ health information has been removed, a utility that overwrites the entire disk drive with “1”s and “0”s must be used.



Policy & Procedure

HIPAA / PRIVACY DESTRUCTION OF PROTECTED HEALTH INFORMATION

FUNCTION

HIPAA

NUMBER

1018

PRIOR ISSUE

EFFECTIVE DATE

10/01/2014

- b. If the computer is being re-deployed internally or disposed of due to obsolescence, the aforementioned utility must be run against the computer's hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.
 - c. If the computer is being disposed of due to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser. This applies to PC workstations, laptops and servers.
2. Compact Disks, Thumb Drives (CDs) and Diskettes: CDs containing resident health information must be cut into pieces or pulverized before disposal.
3. If a service is used for disposal, the vendor should provide a certificate indicating the following:
 - a. Computers and media that were decommissioned have been disposed of in accordance with environmental regulations as computers and media may contain hazardous materials.
 - b. Data stored on the decommissioned computer and/or media was erased or destroyed per the previously stated method(s) prior to disposal.



Policy & Procedure

HIPAA / PRIVACY DESTRUCTION OF PROTECTED HEALTH INFORMATION

FUNCTION HIPAA
NUMBER 1018
PRIOR ISSUE
EFFECTIVE DATE 10/01/2014

This page intentionally left blank.

This page intentionally left blank.