



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

## Section 10

### HIPAA Privacy and Breach

#### 10.1 Privacy Compliance Requirements

In order to comply with the statutory and regulatory requirements of HIPAA, GINA and HITECH and to maintain the privacy of Protected Health Information (PHI) we have implemented policies and procedures to ensure:

- Patients are notified of our privacy practices.
- Employees are trained on our HIPAA Privacy policies and procedures within 30 days of hire or of changes to our procedures.
- Designation of a Privacy Officer committed to overseeing HIPAA Privacy training and education, enforcing policies and procedures and addressing patient requests and complaints.
- Patients have the right to access, receive a copy and to request amendments to their own records.
- Only the minimum necessary PHI is used or disclosed.
- PHI is only used or disclosed when required, permitted or authorized.
- All Business Associates (BAs) have completed a Business Associate Agreement (BAA) with Healthplus Pharmacy & Wellness.
- Patients have the right to authorize or restrict use and disclosure of their PHI.
- Appropriate safeguards are in place to protect health information.
- Prevent intimidation or retaliatory acts against patients or any individual.
- Prohibit requirements for patients to waive their privacy rights.
- Document all HIPAA Privacy transactions and retain records.
- Enforce sanctions and discipline for employees that fail to comply with any HIPAA Privacy policy, procedure or rule.
- Correct any harmful effects of violations of HIPAA Privacy policy, procedure or rule.

What follows are the Policies and Procedures in detail that we have in place to ensure compliance with the requirements listed above. These policies and procedures will guide the daily conduct of employees and will address areas of HIPAA Privacy. We are committed to doing our part to protect patient health information and will continue to update and improve our HIPAA Compliance Program to keep abreast of new laws, regulations, standards and other requirements as necessary.

#### 10.2 Privacy Officer

The Privacy Officer will be selected by the owner of Healthplus Pharmacy & Wellness or the owner may elect to be the Privacy Officer themselves. It is our policy that the Privacy Officer cannot be a subcontracted entity, but must be an employee of Healthplus Pharmacy & Wellness. The Privacy Officer will be responsible, reliable, intelligent, ethical, trustworthy and hard-working. These attributes will be vital to the successful



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

**PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual**

execution of this post. The owner of Healthplus Pharmacy & Wellness may select the same person to fulfill the role of Compliance, Privacy and Security (CPS) Officer.

Healthplus Pharmacy & Wellness's 2024 Privacy Officer is: Vishal Barot

The overarching responsibility of our Privacy Officer is to ensure that we remain compliant with all legal, regulatory, statutory and other requirements set forth by the State and Federal governments relating to privacy.

The Privacy Officer will also serve as our HIPAA Privacy communication hub. All patient requests for privacy forms and complaints will be directed through the Privacy Officer.

Because the duration of tenure of the Privacy Officer may change over time, much of how the Privacy Officer ensures compliance will be left to the discretion of the individual officer. The Privacy Officer's duties in whole may not be delegated to other employees, with only one exception. If the Privacy Officer is required to perform an investigation or tasks which will result in self-policing, the Privacy Officer will surrender their responsibilities to an interim Privacy Officer who has no involvement or conflict; either the owner, or an agent appointed by the owner, for the duration of the investigation.

**The explicit duties of the Privacy Officer include (but are not limited to) the following:**

1. *Implementing the initial HIPAA Privacy education module. This includes:*
  - a. *Making sure all employees successfully complete PAAS National's HIPAA Privacy training program.*
  - b. *Providing employees with training and information on Healthplus Pharmacy & Wellness's specific privacy policies and procedures.*
2. *Investigate and act on any privacy related complaints. Such investigations will be conducted discretely and will respect the confidentiality of information provided by patients or employees.*
3. *Cooperate with potential compliance reviews/investigations by the Department of Health and Human Services, Office for Civil Rights and facilitate any documentation or procedural requests that the OCR makes to the pharmacy. Similarly, the Privacy Officer should collaborate with relevant State agencies or officers in compliance with State privacy laws and regulations.*
4. *Research State laws to identify any regulations that should be added to this policy manual and ensure that all policies and procedures are in accordance with State law.*
5. *Monitor legal and other regulatory developments on a State and Federal level for changes to privacy requirements and make necessary updates to our HIPAA program.*
6. *Maintain documentation for each request, denial, modification, notice, acknowledgement, complaint and corrective actions for a period of at least six years from the date created or the last date used, whichever is later.*
7. *Regularly report to the pharmacy ownership and/or management on the status of HIPAA Privacy implementation and the identification and resolution of potential or actual instances of violations.*
8. *Notify patients, the Secretary of HHS, media and relevant State agencies, as appropriate, any potential privacy violations or breaches according to Federal and State regulations.*



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

9. *Work with the pharmacy's Security Officer to ensure that security policies and procedures support compliance with HIPAA privacy requirements.*

The Privacy Officer will amend this duty list with help from the pharmacy owner in order to define the scope of the officer's responsibilities as circumstances change over time.

### 10.3 Notice of Privacy Practices

Healthplus Pharmacy & Wellness shall provide a written Notice of Privacy Practices (NOPP) to each new patient that we serve via a direct treatment relationship. This shall include any patient for which we have filled a prescription, provided consultation or performed any pharmacy or health care related services. Healthplus Pharmacy & Wellness shall post a copy of our NOPP in a clear and prominent location and on any current or future websites. A copy of our NOPP shall also be provided to any individual or entity that requests a copy.

Healthplus Pharmacy & Wellness's NOPP shall contain our privacy practices as delineated within this Policy and Procedure Manual. It shall also state our desire and duty to protect each patient's privacy and their rights with regard to their Protected Health Information (PHI). No policy or procedure in this manual shall be effective until the effective date of the corresponding NOPP. A copy of each version of our NOPP shall be kept in written or electronic format for a period of at least six years after the last date it was effective.

The NOPP shall be given to each patient when the first service is provided. Healthplus Pharmacy & Wellness shall document that the NOPP has been provided by obtaining acknowledgement from the patient or their personal representative. If the patient is unable or unwilling to provide acknowledgement all good faith attempts to provide the NOPP shall also be documented. Healthplus Pharmacy & Wellness shall use any of the following methods for documenting acknowledgement of receipt of our NOPP:

- Electronic signature capture

Healthplus Pharmacy & Wellness shall not withhold treatment or any health care related service if patients are unable or unwilling to acknowledge receipt of our NOPP.

### 10.4 Minimum Necessary

Healthplus Pharmacy & Wellness and all of its employees shall limit all required, permitted or authorized uses and disclosures of PHI to only the minimum necessary. No employee shall access PHI that is not necessary to complete their assigned job functions. Since assigned job functions may vary by employee and to meet current workload and staffing demands, the following minimums shall apply to the job functions listed:

- Pharmacist – access to any PHI related to the current patient. Shall self-limit access to only the minimum necessary.
- Technician – access to PHI necessary to perform technical functions of preparing and processing prescriptions for pharmacist review.
- Cashier/Bookkeeper – access to PHI related to collection of payment for goods and services provided.
- Delivery Provider – access to PHI related to delivering goods to the appropriate location(s).



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

- Clerk – access to PHI necessary to maintain and order inventory.
- Office/Managerial Staff – access to PHI related to operations and business functions.

If a Healthplus Pharmacy & Wellness employee obtains more than the minimum necessary PHI due to an incidental exposure or an unintentional use or disclosure they shall not further use or disclose such PHI. Any intentional access to PHI that exceeds the minimum necessary shall be addressed in Section 10.12 – Sanctions.

## 10.5 Use and Disclosure

Healthplus Pharmacy & Wellness shall use or disclose PHI only as required, permitted or authorized under HIPAA Rules.

### 10.5.1 Required Use and Disclosure

Healthplus Pharmacy & Wellness shall provide PHI requested by the Secretary of the Department of Health and Human Services (HHS), the Office for Civil Rights (OCR) or any equivalent State agency in the course of any investigation or compliance review. Any such request shall be the responsibility of the Privacy Officer. Prior to use or disclosure, the Privacy Officer shall positively authenticate the identification of the requesting party.

Requests made by the patient or their personal representative shall also be granted by Healthplus Pharmacy & Wellness's Privacy Officer. Such requests shall be made in writing using the appropriate forms found in Appendix B. All request forms shall also be used to document whether such request has been granted or denied and the patient's right to appeal if any.

Forms shall be completed as follows and retained for a period of at least six years after the date last in effect.

**10.5.1.1 Request to Access or Release Protected Health Information:** Shall be submitted prior to granting access or a copy of PHI. Privacy Officer or Pharmacist in Charge, using professional judgment, may waive the requirement of this form if the PHI requested is being released directly to the patient or their personal representative and would not be denied in whole or in part. Records shall be limited to the **Designated Record Set: prescriptions, patient profile and payment records.**

Response to each request must be provided at least 15 days after receipt. Healthplus Pharmacy & Wellness may only delay response for a one time extension of 15 days. Healthplus Pharmacy & Wellness may charge a cost-based fee to provide requested records. Fee shall be limited to the costs of labor for copying, supplies for creating copies (e.g., paper, portable media), postage and costs to prepare a summary or explanation of records if agreed to by the patient. Records shall be provided in the form and format specified, if available. Any denials or delays in providing the requested access or release, shall be provided in writing to the patient or their personal representative on the form. Such requests must be granted in full except for the following denial grounds:

- **Unreviewable Grounds (May not be appealed):** PHI contains psychotherapy notes; PHI is related to a research trial; patient resides in a correctional facility that has denied the request; records are part of a legal action/investigation; records were obtained from a confidential non-health care provider; records are not maintained by Healthplus Pharmacy & Wellness – location of records shall be provided if known.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National<sup>®</sup> Health Care FWA/HIPAA Policy & Procedure Manual

- **Reviewable Grounds (May be appealed):** request is likely to endanger the life or physical safety of the patient or another person; records contain information on another person and access is likely to cause harm to such person; request was made by a personal representative and access is likely to cause harm to the patient or another person

**10.5.1.2 Request to Amend Protected Health Information:** Shall be submitted by the patient or their personal representative to request that their pharmacy records be corrected or amended. The written request must include the reason for the change. Healthplus Pharmacy & Wellness shall have 30 days to respond to an amendment request. Healthplus Pharmacy & Wellness may extend this deadline once for an additional 15 days. Requests shall only be denied if Healthplus Pharmacy & Wellness determines that our records are correct. Any denial or delay shall be documented in writing on the original request form and shall contain the reason for denial or delay. Patients or their personal representatives will have the right to file a Statement of Disagreement against a denial. Healthplus Pharmacy & Wellness reserves the right to file a rebuttal statement to this Statement of Disagreement.

**10.5.1.3 Request an Accounting of Disclosures:** Shall be submitted by the patient or their personal representative to request an accounting of disclosures of their PHI. Healthplus Pharmacy & Wellness shall maintain a record of disclosures for all patients that are not for treatment, payment, health care operations (TPO), public health activities or authorized by the individual. These may include disclosures required by law such as disclosures for health oversight activities (e.g., licensing authorities, Government benefit programs), judicial or administrative proceedings (e.g., court orders, subpoena, discovery request) and for law enforcement activities (e.g., investigations). See Section 10.5.2.5 for full requirements of accounting of disclosures. Healthplus Pharmacy & Wellness shall have 30 days to respond to an accounting of disclosures request. Healthplus Pharmacy & Wellness may extend this deadline once for an additional 15 days. The accounting will be provided in writing on the *Accounting of Disclosures Report* form and shall include the date, the person or entity that received the PHI, a brief description of the PHI disclosed and a brief statement of the purpose for disclosure. Healthplus Pharmacy & Wellness shall provide the first accounting in any 12-month period at no charge. Any subsequent requests for accounting within the 12-month period may be assessed a reasonable cost-based fee. Patient shall be given the opportunity to withdraw or modify such a request to avoid such fee.

**10.5.1.4 Request to Restrict Use and Disclosure:** Shall be submitted by the patient or their personal representative to limit or restrict uses and disclosures of their PHI. This may include specifying which individuals or Covered Entities may not access the patient's records in whole or in part. Covered Entities may not be restricted from access to PHI that is necessary to provide treatment, payment or health care operations or for any use or disclosure that would be required by law. Healthplus Pharmacy & Wellness is not required to agree with restrictions other than to the patient's health plan for payment that was made in full by a person or entity other than the health plan. If Healthplus Pharmacy & Wellness agrees to the restriction, we shall comply with the request unless terminated, required by law or for purposes of emergency treatment. Restrictions may be terminated through the following methods:



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National's Health Care FWA/HIPAA Policy & Procedure Manual

- **Patient Request:** A patient or their personal representative may submit a new *Request to Restrict Use and Disclosure* form in writing to terminate or modify an existing restriction. The patient or their personal representative may also make such a request verbally. Verbal requests shall be recorded on the original request form.
- **Pharmacy Initiated:** Healthplus Pharmacy & Wellness may terminate a restriction by obtaining the patient or their personal representative's verbal agreement and document consent on the original request form. Healthplus Pharmacy & Wellness may also terminate the restriction after notifying the patient or their personal representative that the termination will only apply to PHI created after they have been informed. Again this notification and termination shall be documented on the original request form.

**10.5.1.5 Request for Confidential Communications:** Shall be submitted by the patient or their personal representative to request communication or PHI by alternate means or to alternate locations. Healthplus Pharmacy & Wellness shall not require patient to provide a reason for the request. Alternate locations can include any location that can be accessed by available delivery and telecommunication services. If not specified, such reasonable requests shall be honored until terminated or modified by the patient or their personal representative. Patient or their personal representative shall be made aware that some alternate means, such as email, may not be secure and could endanger the confidentiality of their PHI.

**10.5.2 Permitted Use and Disclosure**

Healthplus Pharmacy & Wellness shall use PHI to conduct its business as permitted under HIPAA regulations without authorization or the patient or their personal representative in the following manner:

**10.5.2.1 To the individual:** PHI may be disclosed by Healthplus Pharmacy & Wellness and its employees and Business Associates directly to the affected patient or their personal representative.

**10.5.2.2 Treatment, Payment and Health Care Operations (TPO):**

- **Treatment:** Healthplus Pharmacy & Wellness shall use PHI to provide treatment. This may involve receiving or sharing information with other health care providers such as physicians and other prescribers. This PHI may be written, verbal, electronic or via facsimile. This will include receiving prescription orders so that we may dispense prescription medications. We may also share PHI with other health care providers that are treating the patient to coordinate the different things they need, such as medications, lab work or other appointments. We may also contact patients to provide treatment-related services, such as refill reminders, treatment alternatives and other health related services that may be of benefit to the patient.
- **Payment:** Healthplus Pharmacy & Wellness shall use PHI to obtain payment. This will include sending claims for payment to insurance and third-party payers. It may also include providing PHI to the payers to resolve issues with payment or claim coverage. The patient or their personal representative may restrict access to their health plan if a person or entity other than their health plan provides payment in full.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

- **Health Care Operations:** Healthplus Pharmacy & Wellness shall use PHI for health care operations. This may include: quality assurance activities; medical review; internal audits; refill reminders; health promotion; financial analysis; and payment reconciliation.

**10.5.2.3 With Opportunity to Agree or Object:** Healthplus Pharmacy & Wellness may disclose PHI to family members, friends or any individual involved with a patient's care. Healthplus Pharmacy & Wellness's employees shall always use professional judgment and experience with common practice to evaluate if the disclosure would be in the best interest of the patient. Healthplus Pharmacy & Wellness shall also honor any requested restrictions that it has agreed to.

**10.5.2.4 Incidental Use and Disclosure:** Healthplus Pharmacy & Wellness is committed to limiting the occurrence and likelihood of incidental uses or disclosures. Please refer to Sections 10.4 – Minimum Necessary and 10.8 – Safeguards.

**10.5.2.5 Law, Death and Public Health Activities:** Healthplus Pharmacy & Wellness shall comply with any uses or disclosures that are required by law or otherwise permitted without the patient's authorization. Healthplus Pharmacy & Wellness's employees shall also record any disclosures that are required to be accounted on the *Accounting of Disclosures Report* form – Appendix B. The following disclosures shall be permitted:

- **Accounting Required:**
  - **Use and Disclosure for a Health Oversight activity:** Healthplus Pharmacy & Wellness may disclose PHI to a health oversight agency to conduct health oversight activities such as: audits; inspections; licensure or disciplinary actions; civil, administrative or criminal investigations, proceedings or actions; or other activities necessary for oversight of the health care system, government benefit or regulatory programs and necessary for determining civil rights law compliance.
  - **Disclosures for Judicial and Administrative proceedings:** Healthplus Pharmacy & Wellness may disclose PHI expressly authorized in an order issued by a court or administrative tribunal.
  - **Disclosures for Law Enforcement purposes:** Healthplus Pharmacy & Wellness may disclose PHI to law enforcement personnel in the following manner:
    - As required by law to report certain types of wounds or other physical injuries (not including victims of abuse, neglect or domestic violence).
    - A court order, court ordered-warrant, subpoena or summons issued by a judicial officer.
    - A grand jury subpoena.
    - An administrative request including an administrative subpoena or summons, a civil or an authorized investigative demand or similar process under law provided that:
      - The information is relevant and material to a legitimate law enforcement inquiry
      - The request is *specific and limited in scope*
      - De-identified information could not be reasonably used.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

- Limited information for identification and location of a suspect, fugitive, material witness or missing person. Must be limited to:
    - Name and address
    - Date and place of birth
    - Social Security number
    - ABO blood type and Rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death
    - A description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.
  - In case of death of patient that may have resulted from criminal conduct
  - Information that Healthplus Pharmacy & Wellness believes to be evidence of criminal conduct against Healthplus Pharmacy & Wellness
- **Accounting NOT Required:**
- **Uses and Disclosures for Public Health activities:** Healthplus Pharmacy & Wellness may use or disclose PHI to an authorized public health entity for the following:
    - To collect or receive such information for preventing or controlling disease, injury or disability, including but not limited to: reporting of disease, injury, vital events (i.e., birth, death); public health surveillance, investigations and interventions.
    - To report child abuse or neglect.
    - To the Food and Drug Administration (FDA) related to the quality, safety and effectiveness of FDA-regulated products or activities such as:
      - To collect and report adverse events, product defects or biological product deviations.
      - To track FDA-regulated products.
      - To enable product recalls, repairs or replacement.
      - To conduct post marketing surveillance.
    - A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.
    - To an employer related to a work-related illness or injury covered under Workers' Compensation
    - To a school regarding a prospective student limited to proof of immunization and either required by law or authorized by the patient or a parent, guardian or legal representative if a minor.
  - **Disclosures about victims of abuse, neglect or domestic violence (non-child):** Where required by law, Healthplus Pharmacy & Wellness may disclose PHI to the appropriate government authority if there is a reasonable belief that the patient is a victim of abuse, neglect or domestic violence. Patient must agree to such disclosure unless:
    - Expressly authorized by statute or regulation.





Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

- Healthplus Pharmacy & Wellness using professional judgment believes the disclosure is necessary to prevent serious harm to the patient or other victims.
- The patient is unable to agree due to incapacity and the receiving agency agrees that PHI shall not be used against the patient and that waiting until patient can provide consent would adversely affect the enforcement activity.

The patient shall be notified immediately that such a report has been or will be made unless Healthplus Pharmacy & Wellness, using professional judgment, believes that the informing the patient would place them at risk or serious harm. If the report is to be given to the patient's personal representative and Healthplus Pharmacy & Wellness believes that the personal representative is responsible for the abuse, neglect or other injury they shall not inform the personal representative.

- **Disclosures for Judicial and Administrative proceedings:** Healthplus Pharmacy & Wellness may disclose PHI in response to a subpoena, discovery request or other lawful process that is not accompanied by a court or administrative tribunal order if:
  - The patient agrees to the use or disclosure; or
  - Reasonable efforts were made to notify by the patient of the disclosure and they did not object or objections were resolved by the court; or
  - Providing a qualified protective order which prohibits the parties from using or disclosing the PHI for any other reason besides the litigation and all PHI shall be returned to Healthplus Pharmacy & Wellness for destruction at the end of the proceedings.
- **Disclosures about Decedents:** Healthplus Pharmacy & Wellness may disclose PHI regarding a deceased patient to the following:
  - **Coroners and Medical Examiners** for purposes of identifying a deceased person, determining a cause of death or other duties authorized by law.
  - **Funeral Directors** as allowed by law and as necessary to carry out their duties with respect to the decedent. PHI may be disclosed in reasonable anticipation of the patient's death.
- **Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation:** Healthplus Pharmacy & Wellness may disclose PHI to an organ procurement organization or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue.
- **Uses and Disclosures for Research:** Healthplus Pharmacy & Wellness may use or disclose PHI for purposes of research upon receipt of patient authorization or a waiver of authorization.
- **Uses and Disclosures to Avert a Serious Threat to Health or Safety:** Healthplus Pharmacy & Wellness may use or disclose PHI, based on law or standards of ethical conduct, that the use or disclosure is necessary to prevent or lessen the serious or imminent threat to the health and safety of a person or the public.
- **Uses and Disclosures for Specialized Government Functions:** Healthplus Pharmacy & Wellness may use or disclose PHI for the following:



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

- **Armed Forces and Foreign Military Personnel:** PHI may be disclosed to the appropriate military command authorities as published in the Federal Register.
- **National Security and Intelligence Activities:** to authorized Federal officials for the conduct of lawful intelligence, counter-intelligence or national security activities.
- **Protective Services for the President and Others:** to authorized Federal officials for the provision of protective services to the President, foreign heads of state or other persons authorized by Federal law.
- **Correctional Institutions and Other Law Enforcement Custodial Situations:** to a correctional institution or to a law enforcement official having lawful custody of an inmate if they represent that the PHI is necessary for:
  - Provision of health care to the inmate
  - Health and safety of the inmate or other inmates
  - Health and safety of the officers or employees at the correctional institution
  - Health and safety of the officers or other persons responsible for transporting the inmate from one institution to another
  - Law enforcement at the correctional institution
  - Administration and maintenance of the safety, security and good order of the correctional institution
- **Disclosures for Workers' Compensation:** Healthplus Pharmacy & Wellness may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness.

**10.5.2.6 De-identified PHI and Limited Data Sets:** Healthplus Pharmacy & Wellness may disclose de-identified PHI and limited data sets as follows:

- **De-identified PHI:** shall consist of health information that does not identify a patient and where there is no reasonable basis to believe that the information could be used to identify a patient. The following identifiers shall be removed:
  - Names
  - All geographic subdivisions smaller than a State, including:
    - Street address
    - City
    - County
    - Precinct
    - Zip code
    - Geocode (GPS coordinates)
  - All elements of dates (except year) for dates directly related to a patient, including:
    - Birth date
    - Admission date
    - Discharge date
    - Date of death



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

- All ages over 89 and all elements of dates (including year) indicative of such age
  - Telephone numbers
  - Fax numbers
  - Email addresses
  - Social Security numbers
  - Medical record numbers
  - Prescription Numbers
  - Health plan ID numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers (including license plates)
  - Device identifiers and serial numbers
  - Web addresses (URLs)
  - IP addresses
  - Biometric identifiers (e.g., fingerprints, voice prints)
  - Full face photos and other comparable images
  - Any other unique identifying number, characteristic or code
- **Limited Data Sets:** shall disclose PHI using limited data sets only for the purposes of research, public health or health care operations after entering into a data use agreement that includes agreement that further use or disclosure is prohibited and excludes the following direct identifiers:
- Names
  - Postal address other than town or city, State and zip code
  - Telephone numbers
  - Fax numbers
  - Email addresses
  - Social Security numbers
  - Medical record numbers
  - Prescription Numbers
  - Health plan ID numbers
  - Account numbers
  - Certificate/license number
  - Vehicle identifiers and serial numbers (including license plates)
  - Device identifiers and serial numbers
  - Web addresses (URLs)
  - IP addresses
  - Biometric identifiers
  - Full face photos and other comparable images

### 10.5.3 Authorized Use and Disclosure

Healthplus Pharmacy & Wellness shall not use or disclose PHI unless otherwise permitted or required without authorization from the patient. Such authorization shall be received in writing from the patient or their personal representative on the *Request to Access or Release Protected Health Information* form – Appendix B. Use or disclosure of PHI containing psychotherapy notes, for marketing or for sale of PHI shall require a



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

separate authorization. Such authorization may not be combined with any other authorization including the Notice of Privacy Practices.

- **Authorization Requirements:** All authorizations must contain the following elements or statements (included in the *Request to Access or Release Protected Health Information* form):
  - What specific PHI is to be used or disclosed
  - Who is authorizing the use or disclosure
  - Who is authorized to receive the PHI
  - A description of the purpose of the authorization
  - An expiration date or event
  - Signature of the patient or their personal representative (and their authority to act on behalf of the patient)
  - Statement of patient's right to revoke the authorization
  - Statement that treatment, payment, enrollment or eligibility for benefits may not be conditioned on patient signing authorization or the consequences if conditions do apply
  - Statement of the potential for PHI to be redisclosed by the recipient since it is no longer protected
- **Selling PHI:** Healthplus Pharmacy & Wellness shall require a separate authorization from patients prior to selling PHI. In addition to the standard authorization requirements, the authorization must also include a statement that Healthplus Pharmacy & Wellness will receive remuneration from a third party in exchange for their PHI. The sale or transfer of Healthplus Pharmacy & Wellness and all its records to a new owner shall not be considered a sale of PHI.
- **Marketing:** Healthplus Pharmacy & Wellness shall require a separate authorization from patients prior to conducting marketing activities that will result in remuneration from a third party. The authorization must include a statement that Healthplus Pharmacy & Wellness will receive remuneration for the marketing activities. Healthplus Pharmacy & Wellness may conduct the following non-marketing activities without authorization:
  - Face-to-face communications
  - Providing a promotional gift of nominal value (e.g., magnet, pen, sticker)
  - Refill reminders
  - Communication regarding a drug the patient is currently being prescribed
  - Treatment of the patient including: case management; care coordination; direct or recommend alternative therapies, treatments, health care providers or settings of care
  - To describe a health-related product or service that is provided by Healthplus Pharmacy & Wellness

## 10.6 Business Associate Agreements

Healthplus Pharmacy & Wellness shall identify all Business Associates (BAs) that may create, receive, maintain or transmit PHI on our behalf. All such BAs shall be required to complete a Business Associate Agreement (BAA) prior to use or disclosure of PHI. All of Healthplus Pharmacy & Wellness's BAs shall require that a BAA be executed with any of their BAs or subcontractors. BAAs shall limit the PHI used or disclosed by BAs to only the minimum necessary which may include a limited data set. BAAs shall also specify how each BA shall protect PHI and notify Healthplus Pharmacy & Wellness of any violations or breaches that occur.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

## 10.7 Privacy Training

***It is our policy to provide employees with the needed information, tools and resources to understand and agree to cooperate with and be actively involved in our HIPAA Privacy efforts. The following procedures are in place:***

1. All employees are provided with an addendum to the Employee Compliance Training Handbook, containing daily policies and procedures. See Section 2.4 for details.
2. All employees must successfully complete the PAAS National® HIPAA Training program at the time of hire (first 30 days) and at least annually thereafter; in addition, employees are provided specific training on our pharmacy's policies and procedures as well as relevant State and local laws pertaining to privacy of health information.

## 10.8 Safeguards

Healthplus Pharmacy & Wellness shall have in place appropriate administrative, technical and physical safeguards to protect PHI. In addition to the safeguards listed in Section 11 of this manual to protect ePHI, Healthplus Pharmacy & Wellness shall implement the following safeguards to protect all PHI:

- Pharmacy has a method to dispose of PHI (i.e. shredder or bonded shredding service)
- All Pharmacy employees dispose of PHI properly (Check general trash bins for unsuspected Protected Health Information)
- Pharmacy has a private consultation area
- Pharmacy verified computer screens or other visual things with PHI are not able to be seen by customers or patients (Stand on the other side of the prescription counter and look in the pharmacy from a patient's perspective)
- Pharmacy assigns unique computer access codes only to those employees authorized to access PHI
- Pharmacy knows which employees have computer access codes
- Unauthorized personnel do not access PHI on computer or borrow access codes
- Pharmacy monitors who accesses what data and that it is appropriate and pertinent to doing their job vs. unauthorized access
- Pharmacy computer back-up tapes or hard drives are encrypted (This offers the pharmacy protections from breach notification requirements in HITECH – Health Information Technology for Economic and Clinical Health Federal Regulation)
- Pharmacy computer back-up tapes or hard drives are stored in a secure locked location
- Access to pharmacy floor space is limited to authorized HIPAA trained employees only

## 10.9 Complaints

Patients that believe their privacy rights or that any Privacy, Security or Breach Rules have been violated have the right to file a complaint with Healthplus Pharmacy & Wellness's Privacy Officer or with the Secretary of Health and Human Services, Office for Civil Rights (OCR). Complaints must be filed in writing and sent via fax, mail or electronically. Patients may use the *HIPAA Patient Complaint* form – Appendix B, *OCR Health*



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National' Health Care FWA/HIPAA Policy & Procedure Manual

*Information Privacy Complaint Form Package or OCR Complaint Portal – <http://www.hhs.gov/ocr>, or in their own written format. Other written formats must include:*

1. Patient's name
2. Full address
3. Telephone number(s)
4. E-mail (if available)
5. Name, full address and telephone number of the person, agency or organization they believe violated their health information privacy rights
6. Brief description of what happened. How, why and when.
7. Any other relevant information
8. Complainant's signature and date of complaint.
9. Name of person you are filing complaint on behalf of (if different)

All complaints filed shall receive a preliminary review by Healthplus Pharmacy & Wellness's Privacy Officer or the owner's designee if the complaint directly relates to the Privacy Officer to determine if a violation may have occurred. If the preliminary review shows that a violation may have occurred, the Privacy Officer or the owner's designee shall conduct a full investigation. Results shall be documented on the *HIPAA Patient Complaint* form and shall contain the relevant facts, efforts to mitigate harm to the patient, sanctions that have been applied or any policies or procedures that need to be revised or updated.

Healthplus Pharmacy & Wellness's Privacy Officer shall coordinate any record requests from OCR needed to conduct an investigation or compliance review related to a complaint submitted to OCR.

## **10.10 Mitigation**

Healthplus Pharmacy & Wellness shall mitigate, to the extent practicable, any harmful effect that is discovered in relation to an unauthorized use or disclosure in violation with these policies and procedures or any HIPAA requirements. This may include but is not limited to Section 10.12 – Sanctions and Section 10.14 – Breach Notification.

## **10.11 Refraining from Intimidating or Retaliatory Acts, Waiver of Rights**

Healthplus Pharmacy & Wellness shall not allow any workforce member to intimidate, threaten, coerce, discriminate against or take any retaliatory action against an individual who chooses to exercise their HIPAA rights. This includes patients or workforce members (whistle blowers) that have filed complaints against Healthplus Pharmacy & Wellness or any of its owners, managers or workforce members.

No patient shall be required to waive their rights under HIPAA rules as a condition of the provision of treatment or payment.

## **10.12 Sanctions**



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

Any employee or workforce member that violates these policies and procedures or any HIPAA requirement shall be sanctioned according to our policies and procedures found in Section 8 of this manual. Any willful or intentional violations may be cause for immediate termination.

## 10.13 Documentation

Healthplus Pharmacy & Wellness shall record and maintain all documentation required under this Section and Section 11 of the Policy and Procedure Manual for a period of at least six years from the date created or the last date in effect, whichever is later. This includes but is not limited to policies and procedures, NOPPs, BAAs, acknowledgements, requests and denials. Documentation may be stored as written or electronic records.

## 10.14 Breach Notification

Any unauthorized acquisition, access, use or disclosure of PHI shall be immediately reported by workforce members to Healthplus Pharmacy & Wellness's Privacy Officer. Such reports shall be assessed upon discovery by Healthplus Pharmacy & Wellness's Privacy and Security Officers to determine if a breach has occurred.

- **Breach Excludes:**

- Any unintentional acquisition, access or use of PHI by an employee or BA if such acquisition, access or use was in good faith and within the scope of authority and is not further used or disclosed in a manner that is not permitted.
- Any inadvertent disclosure from one authorized employee to another authorized employee and the PHI is not further used or disclosed in a manner that is not permitted.
- A disclosure of PHI that the Officers have determined through good faith review that the unauthorized person whom received the disclosure would not reasonably have been able to retain the PHI.

All non-excluded acquisition, access, use or disclosure of PHI shall be considered a breach unless the Officers are able to demonstrate that there is a low probability that the PHI has been compromised based on the following risk assessment factors.

- **Risk Assessment Factors:**

- What was the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification?
- Who was the unauthorized person that received the PHI?
- Was the PHI actually acquired or viewed?
- What measures were implemented to reduce or mitigate the risk of harm to the patient(s)?
- Was the PHI rendered unusable, unreadable or indecipherable (e.g., shredded, encrypted, destroyed, purged) to the unauthorized person through technical or physical process?



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National<sup>®</sup> Health Care FWA/HIPAA Policy & Procedure Manual

Any of the required notifications or details of a breach shall be documented and retained in Healthplus Pharmacy & Wellness's files for a period of at least six years from the date when last effective.

**10.14.1 Notification of Patient**

Following the discovery of a breach of unsecured PHI, Healthplus Pharmacy & Wellness's Privacy Officer shall notify each patient whose PHI is reasonably believed to have been acquired, accessed, used or disclosed as a result of such breach. Notifications shall be provided as soon as possible but no later than 60 days after the discovery of the breach. The contents of the notice shall include:

- A brief description of what happened including the date of breach and the date of discovery, if known.
- A description of the types of unsecured PHI that were involved (e.g., name, social security number, date of birth, prescription numbers)
- Any steps the patient should take to protect themselves from potential harm.
- A brief description of what Healthplus Pharmacy & Wellness is doing to investigate the breach, reduce the harm to the patient and to protect against future breaches.
- The contact information for Healthplus Pharmacy & Wellness's Privacy Officer including phone, email and/or address.

All notices shall be provided in plain language written format and sent via first-class mail to the last known address of the patient or their next of kin if deceased. Information may be provided in one or more mailings as information becomes available. Notice may be sent electronically if the patient has previously requested or agreed to receive communications electronically.

If the patient's contact information is insufficient or out-of-date to provide the notice in written form, a substitute notice may be provided. The following substitute notices may be provided:

- *For fewer than 10 patients:* The patient may be provided a notice by an alternative written form, telephone, or other means.
- *For more than 10 patients:* A conspicuous notice may be posted on the home page of Healthplus Pharmacy & Wellness's website or in major print or broadcast media in the area that patients are likely to reside for a period of 90 days. Such notice shall contain a toll-free number for patients to learn if they are affected by the breach.

If it is urgent that the patient be identified immediately due to an imminent misuse of their PHI, Healthplus Pharmacy & Wellness may provide notice via telephone or other means, as appropriate, in addition to the written notice.

**10.14.2 Notification to the Secretary**

Any incident of breach shall also be reported to the Secretary of Health and Human Services in the manner and form specified by the Secretary on the HHS website.





Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

- **For Breaches involving 500 or more patients:** Notification shall be provided to the Secretary at the same time that notification is provided to the patient. This must be as soon as possible but no later than 60 days after discovery of the breach.
- **For Breaches involving less than 500 patients:** Healthplus Pharmacy & Wellness shall maintain a log or record of breaches that have occurred for the calendar year. A separate notification shall be completed for each breach that occurred within the calendar year. Notification shall be provided to the Secretary no later than 60 days after the end of the calendar year.

**10.14.3 Notification to the Media**

For any breach that involves more than 500 patients that are residents of a State or jurisdiction, Healthplus Pharmacy & Wellness shall notify prominent media outlets within the State or jurisdiction. Notification shall be provided as soon as possible but no later than 60 days after the discovery of the breach. Notification shall include the same required elements as the notification to the patient per *Section 10.14.1*.

**10.14.4 Notification by a Business Associate**

Healthplus Pharmacy & Wellness requires that all of its Business Associates provide notification as soon as possible upon discovery of a breach that involves PHI of Healthplus Pharmacy & Wellness's patients. Our Privacy Officer shall then provide the required notifications to the patient, Secretary and/or media per *Sections 10.14.1-10.14.3*.

**10.14.5 Law Enforcement Delay**

If a law enforcement official states that required notification would impede a criminal investigation or cause harm to national security Healthplus Pharmacy & Wellness shall delay required notifications. If the statement is provided in writing, Healthplus Pharmacy & Wellness shall delay notifications until time of delay has expired. If the statement is provided verbally, Healthplus Pharmacy & Wellness shall document the statement and delay required notification temporarily. Temporary delay shall not exceed 30 days from verbal statement unless a written statement is also provided.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

## Section 11

### HIPAA Security and Other Administrative Simplification

#### 11.1 Security Compliance Requirements

In order to comply with the statutory and regulatory requirements of HIPAA, GINA and HITECH and to maintain the security of electronic Protected Health Information (ePHI) we have implemented policies and procedures to ensure:

- Employees are trained on our HIPAA Security policies and procedures within 30 days of hire or of changes to our procedures.
- Designation of a Security Officer committed to overseeing HIPAA Security training and education, enforcing policies and procedures and evaluating the effectiveness of security measures.
- Appropriate safeguards are in place to protect electronic health information.
- Ensure the confidentiality, integrity and availability of ePHI.
- Protect against any reasonably anticipated threats to the security of ePHI.
- Contingency plans are in place to prepare for emergencies that may affect the security of ePHI.

What follows are the Policies and Procedures in detail that we have in place to ensure compliance with the requirements listed above. These policies and procedures will guide the daily conduct of employees and will address areas of HIPAA Security. We are committed to doing our part to protect patient health information and will continue to update and improve our HIPAA Compliance Program to keep abreast of new laws, regulations, standards and other requirements as necessary.

#### 11.2 Security Officer

The Security Officer will be selected by the owner of Healthplus Pharmacy & Wellness or the owner may elect to be the Security Officer themselves. It is our policy that the Security Officer cannot be a subcontracted entity, but must be an employee of Healthplus Pharmacy & Wellness. The Security Officer will be responsible, reliable, intelligent, ethical, trustworthy and hard-working. These attributes will be vital to the successful execution of this post. The owner of Healthplus Pharmacy & Wellness may select the same person to fulfill the role of Compliance, Privacy and Security (CPS) Officer.

Healthplus Pharmacy & Wellness's 2024 Security Officer is: Vishal Barot

The overarching responsibility of our Security Officer is to ensure that we remain compliant with all legal, regulatory, statutory and other requirements set forth by the State and Federal governments relating to security of ePHI.

Because the duration of tenure of the Security Officer may change over time, much of how the Security Officer ensures compliance will be left to the discretion of the individual officer. The Security Officer's duties



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

in whole may not be delegated to other employees, with only one exception. If the Security Officer is required to perform an investigation or tasks which will result in self-policing, the Security Officer will surrender their responsibilities to an interim Security Officer who has no involvement or conflict; either the owner, or an agent appointed by the owner, for the duration of the investigation.

**The explicit duties of the Security Officer include (but are not limited to) the following:**

1. *Implementing HIPAA Security education. This includes:*
  - a. *Making sure all employees participate in routine security reminder trainings.*
  - b. *Providing employees with training and information on Healthplus Pharmacy & Wellness's specific security policies and procedures.*
2. *Complete the Risk Analysis Worksheet at least annually.*
3. *Investigate and act on any security related incidents. Such investigations will be conducted discretely and will respect the confidentiality of information provided by patients or employees.*
4. *Cooperate with potential compliance reviews/investigations by the Department of Health and Human Services, Office for Civil Rights and facilitate any documentation or procedural requests that the OCR makes to the pharmacy. Similarly, the Security Officer should collaborate with relevant State agencies or officers in compliance with State security laws and regulations.*
5. *Research State laws to identify any regulations that should be added to this policy manual and ensure that all policies and procedures are in accordance with State law.*
6. *Monitor legal and other regulatory developments on a State and Federal level for changes to HIPAA security requirements and make necessary updates to our HIPAA program.*
7. *Maintain documentation for each security incident, information system review, access request, risk analysis or other required report for a period of at least six years from the date created or the last date used, whichever is later.*
8. *Regularly report to the pharmacy ownership and/or management on the status of HIPAA Security implementation and the identification and resolution of potential or actual instances of violations.*
9. *Work with the pharmacy's Privacy Officer to ensure that privacy policies and procedures support compliance with HIPAA security requirements.*
10. *Review and process requests to access ePHI or areas where ePHI is available.*
11. *Conduct and maintain an accurate and thorough inventory of all hardware and software used to create, store or transmit ePHI.*
12. *Review and test contingency plans on a routine basis.*

The Security Officer will amend this duty list with help from the pharmacy owner in order to define the scope of the officer's responsibilities as circumstances change over time.

## **Administrative Safeguards**

### **11.3 Security Management Process**

The following policies and procedures are implemented to prevent, detect, contain and correct security violations.



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National<sup>®</sup> Health Care FWA/HIPAA Policy & Procedure Manual

**11.3.1 Risk Analysis:** Healthplus Pharmacy & Wellness's Security Officer shall conduct an accurate and thorough assessment of the potential threats, vulnerabilities and the associated risks to the confidentiality, integrity and availability of ePHI. This risk analysis shall be documented on the *Risk Analysis Worksheet* and retained for at least six years. A new risk analysis shall be completed at least annually or whenever there are significant changes to the information systems or security policies and procedures.

**11.3.2 Risk Management:** Upon completion of the Risk Analysis, the Security Officer shall convene a Risk Management workgroup that shall include at least the Security Officer, Privacy Officer, Owner and/or Manager. The workgroup shall conduct the following activities:

1. Each of the risks identified in the Risk Analysis shall be prioritized based upon potential impact.
2. Any recommended security measures that have been implemented to reduce or mitigate risks shall be evaluated.
3. Conduct a cost-benefit analysis of potential security measures to further reduce risks or their impact.
4. Select controls that are reasonable and appropriate to implement.
5. Assign to Security Officer responsibility to determine the resources, schedule and maintenance requirements for each control.
6. Complete a *Security Implementation Plan Worksheet – Appendix B* to document the implementation plan and progress.
7. Evaluate the progress of implementation plans and the effectiveness of security measures.
8. Implement all security controls.
9. Conduct a new Risk Analysis at least annually or whenever significant changes have been made to information systems software, hardware or security controls.
10. Maintain documentation of all Risk Analysis and Security Implementation Plans for a period of at least six years.

**11.3.3 Sanction Policy:** All of Healthplus Pharmacy & Wellness's employees are required to comply with all policies and procedures to protect the security of ePHI. Any employee that violates these policies and procedures or any other Federal or State law in regards to the security of ePHI shall be subject to appropriate sanctions. See Section 8 of this Policy & Procedure Manual.

**11.3.4 Information System Activity Review:** Healthplus Pharmacy & Wellness's Security Officer shall review information system activity at least every 90 days. Such activity may include but is not limited to audit logs, access reports and security incident tracking reports. Reviews conducted shall be documented on the *Information System Activity Review Log – Appendix B*.

## 11.4 Workforce Security

The following policies and procedures are implemented to ensure that employees, volunteers and students have appropriate access to ePHI and that prevent workforce members who should not have access from obtaining access.



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

- 11.4.1 Authorization and/or Supervision:** Each workforce member of Healthplus Pharmacy & Wellness shall request authorization to access ePHI or areas where ePHI may be accessed by completing an *Employee Request for Access – Appendix B* form. Requests forms must then be provided to the member's direct supervisor or manager to provide validation of employment and the access that member will require to perform their designated job functions. The completed request form shall be submitted to the Security Officer for final review.
- 11.4.2 Workforce Clearance Procedures:** The Security Officer shall only grant access to a workforce member that has submitted a completed and validated *Employee Request for Access – Appendix B* form. The Security Officer shall review each submitted form and determine if the requested access is appropriate for the member to complete their job functions. Security Officer shall also ensure that access is not granted until member has completed all required HIPAA training modules. Requests shall be documented as approved or denied and retained for at least six years after the last effective date.
- 11.4.3 Termination Procedures:** Security Officer shall immediately terminate a workforce member's authorization to ePHI or areas where ePHI may be accessed upon termination of employment or a change in job functions that requires less or no access to ePHI. Owner, Manager and/or Security Officer may elect to terminate authorization in advance of termination and/or upon reasonable belief that member may be violating security policies. All logins and passwords shall be deactivated and member shall return any keys or badges that allow access. Termination including the return of keys shall be documented on the *Employee Request for Access – Appendix B* form and retained for six years.

## 11.5 Information Access Management

- 11.5.1 Isolating Health Care Clearinghouse Functions:** Healthplus Pharmacy & Wellness does not operate a health care clearinghouse or perform health care clearinghouse functions.
- 11.5.2 Access Authorization:** Healthplus Pharmacy & Wellness shall grant access to ePHI in the following manner:
- Workstation access is limited by user or user role using appropriate login and password (i.e., each computer requires login by an authorized user)
  - Software access is limited by user or user role using appropriate login and password (i.e., applications like your pharmacy software require login)
  - Specific data or processing steps are limited by user or user role using appropriate login and password (e.g., allowing technicians to complete data entry but a delivery driver can only look at patient address and phone)
- 11.5.3 Access Establishment and Modification:** Security Officer shall establish or modify access to ePHI upon approval of a completed and validated *Employee Request for Access* form and in accordance with Section 11.5.2 to the manner that access shall be granted.

## 11.6 Security Awareness and Training



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

The following policies and procedures are implemented to create a security awareness and training program for all members of Healthplus Pharmacy & Wellness's workforce including management.

**11.6.1 Security Reminders:** Healthplus Pharmacy & Wellness's Security Officer shall provide security updates and reminders to all workforce members at least every 90 days. They will receive Security reminders in the following manner: a personal notice, given to each employee or by other means, including email. These reminders may include: why security is important, steps that can reduce risks, possible threats, setting strong passwords or other similar topics.

**11.6.2 Protection from Malicious Software:** Healthplus Pharmacy & Wellness shall implement the following procedures to guard against, detect and report malicious software:

- A hardware firewall is installed on the network to prevent unauthorized access from outside the internal network

**11.6.3 Log-in Monitoring:** Employees are required to only use their assigned unique log-in. Healthplus Pharmacy & Wellness shall implement the following procedures to monitor log-in attempts and report discrepancies:

- Software blocks further log-in attempts after a limited number of failed attempts

**11.6.4 Password Management:** Healthplus Pharmacy & Wellness requires that employees create strong passwords that are difficult to guess or decipher. Such passwords shall be required to be created within the following **minimum** guidelines:

- Include a combination of upper case and lower case letters
- Include at least one number

To ensure continued strength of passwords employees are required to change their password at least every 180 days. The following additional safeguards shall also be implemented:

- Each employee has their own unique login and password
- Passwords are not shared or revealed with others
- Passwords are not written down
- Password entry is masked (displays as \*\*\*\* or similar) or not displayed
- Passwords are not reused
- Password is linked to a biometric scan (e.g., fingerprint, retina scan, palm vein scan)

## 11.7 Security Incident Procedures

Any suspected or known incidents including breach, exploited vulnerability or violations of these policies and procedures or any Federal or State security rule must be reported immediately to the Security Officer. Incidents shall be submitted in writing on the *Security Incident Report* form or if verbally submitted transcribed onto the same form. All incidents shall be fully investigated and documented. The Security Officer shall work with the Privacy Officer to mitigate any harm the incident may cause. Incidents may be



Healthplus Pharmacy & Wellness  
 NCPDP: 2589919  
 238 S Pearson Rd  
 Pearl, MS 392085637  
 Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

referred to the Risk Management workgroup to evaluate and conduct an additional Risk Analysis. The Security Officer may implement additional policies or procedures to prevent future incidents.

## 11.8 Contingency Plan

Healthplus Pharmacy & Wellness shall implement the following policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI.

**11.8.1 Data Backup Plan:** All data that contains ePHI shall have an exact retrievable copy created. Such backups shall be created through the following procedures:

- Data is backed up onto another server or hard drive that is located in a secure offsite location

**11.8.2 Disaster Recovery Plan:** If a disaster or emergency occurs that damages the systems that contain ePHI, the following procedures shall be implemented to restore lost ePHI. Since such disasters could also damage written or electronically stored versions of this Policy and Procedure Manual, copies of Healthplus Pharmacy & Wellness's Disaster Recovery Plan shall be maintained and stored in the following alternate locations and/or with the following personnel:

- Pharmacy, Main Office- Owner, Security Office will also have copies.

Systems that have experienced total or partial loss of data shall have data restored from the appropriate backup created per Section 11.8.1 of this manual. This restoration procedure shall be as follows:

- Call pioneer rx help line

If the disaster or emergency has damaged or destroyed the hardware or software needed to access the ePHI, the following hardware and software shall be required for data to be restored:

- Pioneer RX

If the pharmacy has been damaged or destroyed by the disaster or emergency and is rendered inaccessible, the following alternate locations may be utilized to recover or restore lost ePHI:

- Main owner office

**11.8.3 Emergency Mode Operation Plan:** In case of an emergency that allows for continued critical business operations, Healthplus Pharmacy & Wellness shall begin operation in Emergency Mode. Only critical business operations shall be conducted while in Emergency Mode to protect the security of ePHI. Healthplus Pharmacy & Wellness shall require that the following software and/or hardware be operational in order to operate in Emergency Mode:

- Work Station, Pharmacy Application, Internet, Printer



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

## PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

Healthplus Pharmacy & Wellness must also have access to the following data in written or electronic format for Emergency Mode operations:

- Refill History, Patient Demographics, Payment History

Healthplus Pharmacy & Wellness shall cease or not initiate operating in Emergency Mode if the following threshold has been exceeded to prevent the emergency from jeopardizing the continued security of ePHI:

- Loss of Power, Server Offline, Pharmacy Software Not Accessible, Natural Disaster/Act of God, Access to Medications.

**11.8.4 Testing and Revision Procedures:** Healthplus Pharmacy & Wellness shall conduct a test of its Data Backup, Disaster Recovery and Emergency Mode Operation plans at least once a year or as needed to accommodate any changes in policy, procedure, software and/or hardware. Plans shall be revised as appropriate if deficiencies are found in any of the contingency plans. Testing may include but is not limited to: verifying that backup contains exact copy of data; validating that backup can be restored; that updated copies of contingencies plans are kept at alternate locations; critical business operations can continue; and/or security of ePHI is maintained.

## 11.9 Evaluation

Healthplus Pharmacy & Wellness's Security Officer shall conduct an evaluation of all policies and procedures at least annually. This evaluation shall be based on any environmental or operational changes that may affect the security of ePHI.

## 11.10 Business Associate Contracts and Other Arrangements

Healthplus Pharmacy & Wellness may permit a Business Associate (BA) to create, receive, maintain or transmit ePHI on our behalf only after they have completed a Business Associate Agreement (BAA) that contains their assurance that the security of ePHI shall be appropriately safeguarded. BAs must also ensure that their subcontractors or other BAs must also appropriately safeguard ePHI.

## Physical Safeguards

### 11.11 Facility Access Controls

Healthplus Pharmacy & Wellness shall implement the following policies and procedures to limit physical access to ePHI and facility or facilities in which they are housed.

**11.11.1 Contingency Operations:** No employee or patient shall be allowed access to pharmacy or pharmacy areas during an emergency until the Security Officer has determined that the security of ePHI would not be compromised. Only the critical workforce members will be allowed during Emergency Mode Operation.





Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National<sup>®</sup> Health Care FWA/HIPAA Policy & Procedure Manual

**11.11.2 Facility Security Plan:** Healthplus Pharmacy & Wellness shall have the following safeguards in place to protect the security of the pharmacy from unauthorized physical access, tampering or theft:

- Pharmacy has barriers such as doors, gates or walls to block physical access without proper keys
- Pharmacy has an alarm to detect and deter unauthorized access
- Hardware containing ePHI is secured or locked to its location within the pharmacy to prevent removal
- Pharmacy has panic alarms to notify authorities of a forced unauthorized access
- Pharmacy has a video recording system

**11.11.3 Access Control and Validation Procedures:** Healthplus Pharmacy & Wellness shall implement the following policies and procedures to control and validate a person's access to the pharmacy based on their role or function, including visitor control and control of access to software programs for testing and revision:

- Software access shall not be granted to non-employees
- Representatives of other Covered Entities or their Business Associates shall not be granted access to ePHI or areas where ePHI may be accessed unless under direct supervision of an authorized user who shall provide access only to the minimum ePHI necessary
- All authorized persons shall prominently display authenticated identification while in pharmacy areas
- Access required by State or Federal law shall be honored once requirements and identification have been validated and authenticated
- Non-employee visitors (e.g., volunteers, students, contract workers, media) shall only be granted supervised access to pharmacy areas upon completion of HIPAA training
- Patients may only be authorized in areas that do not have access to ePHI or are intended to provide clinical services to patients (e.g., counseling rooms, exam rooms, vaccination lounges)

**11.11.4 Maintenance Records:** Healthplus Pharmacy & Wellness's Security Officer shall maintain records of all repairs and modifications to the physical components of the pharmacy related to security such as walls, doors, locks and hardware. All such records shall be documented on the *Maintenance Record Log* form and retained for at least six years.

**11.11.5 Audio, Video, and Social Media:** It is Healthplus Pharmacy & Wellness's policy not to permit any unauthorized video or audio recording in the pharmacy area by employees, pharmacy customers, or other people. Individuals are strictly forbidden from taking any pictures, videos, or audio recordings on personal devices.

Healthplus Pharmacy & Wellness uses the following measures to mitigate video and/or audio PHI breaches:

- Staff awareness and training



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National^ Health Care FWA/HIPAA Policy & Procedure Manual

If someone is suspected of violating the policy, management will approach the individual, discuss the policy, and verify that no unauthorized recording has occurred. If a recording exists, we will request its immediate removal and verification that it has been deleted from the device – when possible.

Should an individual post a video or audio recording from our pharmacy disclosing Protected Health Information on a social media platform, we will make a prompt request to that platform for its removal. Additionally, we will ban the offending individual from the pharmacy.

If applicable, our social media page(s) will be handled only by HIPAA-trained, and trusted, individuals within the pharmacy. PHI will never be used or disclosed on social media, including pictures with patients, without the expressed, written consent of the patient. Should a patient wish to file a grievance about a breach of privacy, we will instruct them to fill out a HIPAA Patient Compliant form (found in Appendix B).

## 11.12 Workstation Use and Security

Healthplus Pharmacy & Wellness shall implement the following physical safeguards to protect workstations from unauthorized use or access:

- Workstations are kept in secure pharmacy areas

## 11.13 Device and Media Controls

The following policies and procedures shall govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a pharmacy and the movement of these items within the pharmacy.

**11.13.1 Disposal:** No hardware or electronic media shall be disposed of until it has been properly purged of ePHI or destroyed. Healthplus Pharmacy & Wellness shall require the following:

- Media is shredded, pulverized or disintegrated into particles that are less than 25 square millimeters

**11.13.2 Media Reuse:** No hardware or electronic media shall be reused until it has been properly cleared or purged of ePHI. Hardware or electronic media that is being reused internally may be cleared or purged using the following:

- Media is purged of ePHI using manufacturer's factory reset procedures

Hardware or electronic media that is being reused externally (returned to a vendor, donated or for employee personal use) must be purged using the following:

- Media is purged of ePHI using manufacturer's factory reset procedures
- Media that cannot be securely purged shall be processed for disposal



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

2024

PAAS National® Health Care FWA/HIPAA Policy & Procedure Manual

**11.13.3 Accountability:** Healthplus Pharmacy & Wellness's Security Officer shall maintain a record of the movements of hardware and electronic media and any person responsible for such items on the *Hardware & Media Inventory – Appendix B* form. This may include but not be limited to portable media such as memory cards or sticks, thumb drives, backup tapes, portable hard drives, copiers, fax machines and laptops or other hardware such as workstations, routers, printers and servers. Other electronic media or hardware may not be permitted in the pharmacy including personal media or cell phones unless necessary to perform authorized job functions.

**11.13.4 Data Backup and Storage:** A retrievable, exact copy shall be made prior to movement of any hardware that contains ePHI.

## Technical Safeguards

### 11.14 Access Control

**11.14.1 Unique User Identification:** Healthplus Pharmacy & Wellness's Security Officer shall assign a unique name and/or number for identifying and tracking all authorized users or software applications that access ePHI.

**11.14.2 Emergency Access Procedure:** In the case of an emergency Healthplus Pharmacy & Wellness's Security Officer shall obtain necessary ePHI by implementing the contingency plans as specified in Section 11.8 of this Policy and Procedure Manual.

**11.14.3 Automatic Logoff:** Electronic sessions of software applications or workstations shall be terminated automatically after a period of inactivity of Terminated manually by user. Evaluating for future implementation..

**11.14.4 Encryption and Decryption:** Healthplus Pharmacy & Wellness shall implement the following mechanisms to encrypt and decrypt ePHI:

- Encryption is not deemed appropriate at this time due to small volume of ePHI. Evaluating for future implementation.

### 11.15 Security Audit Controls

Healthplus Pharmacy & Wellness shall use the following software and procedural mechanisms to record and examine activity in information systems that access ePHI:

- Server tracks user login and activity

### 11.16 Integrity

Healthplus Pharmacy & Wellness shall use the following electronic mechanisms to ensure that ePHI has not been altered or destroyed in an unauthorized manner:



Healthplus Pharmacy & Wellness  
NCPDP: 2589919  
238 S Pearson Rd  
Pearl, MS 392085637  
Version Date: 11-23-2018

**2024**

PAAS National\* Health Care FWA/HIPAA Policy & Procedure Manual

- Software tracks all alteration and deletion for review of appropriateness

### 11.17 Person or Entity Authentication

Healthplus Pharmacy & Wellness shall use any of the following procedures to verify that a person or entity that is seeking access to ePHI is the one claimed:

- A valid, unexpired Government issued photo ID
- Biometric scan (e.g., fingerprint, retina scan, palm vein scan)

### 11.18 Transmission Security

**11.18.1 Integrity Controls:** Healthplus Pharmacy & Wellness shall use the following security measures to ensure that transmitted ePHI is not improperly modified without detection until disposed of:

- Transmission is made directly to the recipient, processor or switch and not routed through an unsecured or open network
- Response is required from recipient, processor or switch that confirms data being transmitted

**11.18.2 Encryption:** Healthplus Pharmacy & Wellness shall use the following mechanisms to encrypt ePHI for transmission:

- Approved HIPAA transaction standards are used with required encryption
- Email shall not be used for transmitting ePHI unless patient has requested use of email for confidential communication and has acknowledged that email may not be secure
- Website applications that collect ePHI (e.g., refill requests, messages) shall be encrypted

### 11.19 Other Administrative Simplification Rules

Healthplus Pharmacy & Wellness shall comply with all of the required standard identifiers, transactions and code sets for HIPAA protected transactions. Healthplus Pharmacy & Wellness shall also require all Business Associates to also comply with these standards prior to any published compliance date. This shall include the use of the following standards:

- **Standard Unique Health Identifier for Providers** – National Provider Identifier (NPI)
- **Standard Unique Health Identifier for Health Plans** – Health Plan Identifier (HPID)
- **Standard Unique Employer Identifier** – Employer Identification Number (EIN)