

Original Effective Date: April 14, 2003

A federal regulation, known as the "HIPAA Privacy Rule," requires that we provide detailed notice in writing of our privacy practices. We know this Notice is long. The HIPAA Privacy Rule requires us to address many specific things in this Notice.

I. OUR COMMITMENT TO PROTECTING HEALTH INFORMATION ABOUT YOU

In this Notice, we describe the ways we may use and disclose health information about our patients. The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient, or where there is a reasonable basis to believe the information can be used to identify a patient. This information is called "protected health information" or "PHI." This Notice describes your rights as our patient and our obligations regarding the use and disclosure of PHI. We are required by law to:

- Maintain the privacy of PHI about you;
- Give you this Notice of our legal duties and privacy practices with respect to PHI; and
- Comply with the terms of our Notice of Privacy Practices that is currently in effect.

As permitted by the HIPAA Privacy Rule, we reserve the right to make changes to this Notice and to make such changes effective for all PHI we may already have about you. If and when this Notice is changed, we will post a copy in our office in a prominent location. We will also provide you with a copy of the revised Notice upon your request made to our Privacy Official.

You will be asked to sign a form to show that you received this Notice. Even if you do not sign this form, we will still provide you with treatment.

II. HOW WE MAY USE AND DISCLOSE PROTECTED HEALTH INFORMATION ABOUT YOU FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

The following categories describe the different ways we may use and disclose PHI for treatment, payment, or health care operations without your consent or authorization. The examples included in each category do not list every type of use or disclosure that may fall within that category.

Treatment: We may use and disclose PHI about you to provide, coordinate, or manage your health care and related services. We may consult with other health care providers regarding your treatment, and coordinate and manage your health care with others. For example, we may use and disclose PHI when you need a prescription, lab work, an X-ray, or other health care services. In addition, we may use and disclose PHI about you when referring you to another health care provider. For example, if you are referred to another physician, we may disclose PHI to your new physician regarding whether you are allergic to any medications. In emergencies, we may use and disclose PHI to provide the treatment you need.

We may also disclose PHI about you for the treatment activities of another health care provider. For example, we may send a report about you to a physician that we refer you to so that the other physician may treat you.

Payment: We may use and disclose PHI so that we can bill and collect payment for the treatment and services provided to you. Before providing treatment or services, we may share details with your health plan concerning the services you are scheduled to receive. For example, we may ask for payment approval from your health plan before we provide care or services. We may use and disclose PHI to find out if your health plan will cover the cost of care and services we provide. We may use and disclose PHI to confirm you are receiving the appropriate amount of care to obtain payment for services. We may use and disclose PHI for billing, claims management, and collection activities. We may disclose PHI to insurance companies providing you with additional coverage.

We may also disclose PHI to another health care provider or to a company or health plan required to comply with the HIPAA Privacy Rule for the payment activities of that health care provider, company, or health plan. For example, we may allow a health insurance company to review PHI for the insurance company's activities to determine the insurance benefits to be paid for your care.

Health Care Operations: We may use and disclose PHI in performing business activities that are called health care operations. Health care operations include doing things that allow us to improve the quality of care we provide and to reduce health care costs. We may use and disclose PHI about you in the following health care operations:

- Reviewing and improving the quality, efficiency, and cost of care that we provide to our patients. For example, we may use PHI about you to develop ways to assist our physicians and staff in deciding how we can improve the medical treatment we provide to others.
- Improving health care and lowering costs for groups of people who have similar health problems and helping to manage and coordinate the care for these groups of people. We may use PHI to identify groups of people with similar health problems to give them information, for instance, about treatment alternatives and educational classes
- Reviewing and evaluating the skills, qualifications, and performance of health care providers taking care of you and our other patients.
- Providing training programs for students, trainees, health care providers, or non-health care professionals (for example, billing personnel) to help them practice or improve their skills.
- Cooperating with outside organizations that assess the quality of the care that we provide.
- Cooperating with outside organizations that evaluate, certify, or license health care providers or staff in a particular field or specialty. For example, we may use or disclose PHI so that one of our nurses may become certified as having expertise in a specific field of nursing.
- Cooperating with various people who review our activities. For example, PHI may be seen by doctors reviewing the services provided to you, and by accountants, lawyers, and others who assist us in complying with the law and managing our business.
- Assisting us in making plans for our practice's future operations.
- Resolving grievances within our practice.
- Business planning and development, such as cost-management analyses.
- Business management and general administrative activities of our practice, including managing our activities related to complying with the HIPAA Privacy Rule and other legal requirements.
- Creating "de-identified" information that is not identifiable to any individual, and disclosing PHI to a business associate for the purpose of creating de-identified information, regardless of whether we will use the de-identified information.

- Creating a “limited data set” of information that does not contain information directly identifying a patient. Our ability to disclose this information to others under limited conditions is discussed later in this Notice.

If another health care provider, company, or health plan that is required to comply with the HIPAA Privacy Rule also has or once had a relationship with you, we may disclose PHI about you for certain health care operations of that health care provider or company. For example, such health care operations may include: reviewing and improving the quality, efficiency, and cost of care provided to you; reviewing and evaluating the skills, qualifications, and performance of health care providers; providing training programs for students, trainees, health care providers, or non-health care professionals; cooperating with outside organizations that evaluate, certify, or license health care providers or staff in a particular field or specialty; and assisting with legal compliance activities of that health care provider or company.

We may also disclose PHI for the health care operations of any “organized health care arrangement” in which we participate. An example of an organized health care arrangement is the joint care provided by a hospital and the physicians who see patients at the hospital.

Communication From Our Office: We may contact you to remind you of appointments and to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you.

OTHER USES AND DISCLOSURES WE CAN MAKE WITHOUT YOUR WRITTEN AUTHORIZATION FOR WHICH YOU HAVE THE OPPORTUNITY TO AGREE OR OBJECT

Individuals Involved in Your Care or Payment for Your Care: We may use and disclose PHI about you in some situations where you have the opportunity to agree or object to certain uses and disclosures of PHI about you. If you do not object, we may make these types of uses and disclosures of PHI.

- We may disclose PHI about you to your family member, close friend, or any other person identified by you if that information is directly relevant to the person’s involvement in your care or payment for your care.
- If you are present and able to consent or object (or if you are available in advance), then we may only use or disclose PHI if you do not object after you have been informed of your opportunity to object.
- If you are not present or you are unable to consent or object, we may exercise professional judgment in determining whether the use or disclosure of PHI is in your best interests. For example, if you are brought into this office and are unable to communicate normally with your

physician for some reason, we may find it is in your best interest to give your prescription and other medical supplies to the friend or relative who brought you in for treatment.

- We may also use and disclose PHI to notify such persons of your location, general condition, or death. We also may coordinate with disaster relief agencies to make this type of notification.
- We may also use professional judgment and our experience with common practice to make reasonable decisions about your best interests in allowing a person to act on your behalf to pick up filled prescriptions, medical supplies, X-rays, or other things that contain PHI about you.

OTHER USES AND DISCLOSURES WE CAN MAKE WITHOUT YOUR WRITTEN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT

We may use and disclose PHI about you in the following circumstances without your authorization or opportunity to agree or object, provided that we comply with certain conditions that may apply.

Required By Law: We may use and disclose PHI as required by federal, state, or local law to the extent that the use or disclosure complies with the law and is limited to the requirements of the law.

Public Health Activities: We may use and disclose PHI to public health authorities or other authorized persons to carry out certain activities related to public health, including the following activities:

- To prevent or control disease, injury, or disability;
- To report disease, injury, birth, or death;
- To report child abuse or neglect;
- To report reactions to medications or problems with products or devices regulated by the federal Food and Drug Administration (FDA) or other activities related to quality, safety, or effectiveness of FDA-regulated products or activities;
- To locate and notify persons of recalls of products they may be using;
- To notify a person who may have been exposed to a communicable disease in order to control who may be at risk of contracting or spreading the disease; or
- To report to your employer, under limited circumstances, information related primarily to workplace injuries or illnesses, or workplace medical surveillance.

Abuse, Neglect, or Domestic Violence: We may disclose PHI in certain cases to proper government authorities if we reasonably believe that a patient has been a victim of domestic violence, abuse, or neglect.

Health Oversight Activities: We may disclose PHI to a health oversight agency for oversight activities including, for example, audits, investigations, inspections, licensure and disciplinary activities, and other activities conducted by health oversight agencies to monitor the health care system, government health care programs, and compliance with certain laws.

Lawsuits and Other Legal Proceedings: We may use or disclose PHI when required by a court or administrative tribunal order. We may also disclose PHI in response to subpoenas, discovery requests, or other required legal process when efforts have been made to advise you of the request or to obtain an order protecting the information requested.

Law Enforcement: Under certain conditions, we may disclose PHI to law enforcement officials for the following purposes where the disclosure is:

- About a suspected crime victim if, under certain limited circumstances, we are unable to obtain a person's agreement because of incapacity or emergency;
- To alert law enforcement of a death that we suspect was the result of criminal conduct;
- Required by law;
- In response to a court order, warrant, subpoena, summons, administrative agency request, or other authorized process;
- To identify or locate a suspect, fugitive, material witness, or missing person;
- About a crime or suspected crime committed at our office; or
- In response to a medical emergency not occurring at the office, if necessary to report a crime, including the nature of the crime, the location of the crime or the victim, and the identity of the person who committed the crime.

Coroners, Medical Examiners, Funeral Directors: We may disclose PHI to a coroner or medical examiner to identify a deceased person and determine the cause of death. In addition, we may disclose PHI to funeral directors, as authorized by law, so that they may carry out their jobs.

Organ and Tissue Donation: If you are an organ donor, we may use or disclose PHI to organizations that help procure, locate, and transplant organs in order to facilitate an organ, eye, or tissue donation and transplantation.

Research: We may use and disclose PHI about you for research purposes under certain limited circumstances. We must obtain a written authorization to use and disclose PHI about you for research purposes, except in situations where a research project meets specific, detailed criteria established by the HIPAA Privacy Rule to ensure the privacy of PHI.

To Avert a Serious Threat to Health or Safety: We may use and disclose PHI about you in limited circumstances when necessary to prevent a threat to the health or safety of a person or to the public. This disclosure can only be made to a person who is able to help prevent the threat.

Specialized Government Functions: Under certain conditions, we may disclose PHI:

- For certain military and veteran activities, including determination of eligibility for veterans benefits and where deemed necessary by military command authorities;
- For national security and intelligence activities;
- To help provide protective services for the President of the United States and others;

- For the health or safety of inmates and others at correctional institutions or other law enforcement custodial situations or for general safety and health related to correctional facilities.

Workers' Compensation: We may disclose PHI as authorized by workers' compensation laws or other similar programs that provide benefits for work-related injuries or illness.

Disclosures Required by HIPAA Privacy Rule: We are required to disclose PHI to the Secretary of the United States Department of Health and Human Services when requested by the Secretary to review our compliance with the HIPAA Privacy Rule. We are also required in certain cases to disclose PHI to you upon your request to access PHI or for an accounting of certain disclosures of PHI about you (these requests are described in Section III of this Notice).

Incidental Disclosures: We may use or disclose PHI incidents for a use or disclosure permitted by the HIPAA Privacy Rule so long as we have reasonably safeguarded the information against such incidental uses and disclosures as well as limiting the recipient to the minimum necessary information.

Limited Data Set Disclosures: We may use or disclose a limited data set (PHI that has certain identifying information removed) for the purposes of research, public health, or health care operations. This information may only be disclosed for research, public health, and health care operations purposes. The person receiving the information must sign an agreement to protect the information.

OTHER USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REQUIRE YOUR AUTHORIZATION

All other uses and disclosures of PHI about you will only be made with your written authorization. If you have authorized us to use or disclose PHI about you, you may later revoke your authorization at any time, except to the extent we have taken action based on the authorization.

III. YOUR RIGHTS REGARDING PROTECTED HEALTH INFORMATION ABOUT YOU

Under federal law, you have the following rights regarding PHI about you:

Right to Request Restrictions: You have the right to request additional restrictions on the PHI that we may use or disclose for treatment, payment, and health care operations. You may also request additional restrictions on our disclosure of PHI to certain individuals involved in your care that otherwise are permitted by the Privacy Rule. We are not required to agree to your request. If we do agree to your request, we are required to comply with our agreement except in certain cases, including where the information is needed to treat you in the case of an emergency. To request restrictions, you must make your request in writing to our Privacy Official. In your request, please include (1) the information that you want to restrict; (2) how you want to restrict the information (for example, restricting use to this office, only restricting disclosure to persons outside this office, or restricting both); and (3) to whom you want those restrictions to apply.

Right to Receive Confidential Communications: You have the right to request that you receive communications regarding PHI in a certain manner or at a certain location. For example, you may request that we contact you at home, rather than at work. You must make your request in writing. You must specify how you would like to be contacted (for example, by regular mail to your post office box and not your home). We are required to accommodate only reasonable requests.

Right to Inspect and Copy: You have the right to request the opportunity to inspect and receive a copy of PHI about you in certain records that we maintain. This includes your medical and billing records but does not include psychotherapy notes or information gathered or prepared for a civil, criminal, or administrative proceeding. We may deny your request to inspect and copy PHI only in limited circumstances. To inspect and copy PHI, please contact our Privacy Official. If you request a copy of PHI about you, we may charge you a reasonable fee for the copying, postage, labor, and supplies used in meeting your request.

Right to Amend: You have the right to request that we amend PHI about you as long as such information is kept by or for our office. To make this type of request, you must submit your request in writing to our Privacy Official. You must also give us a reason for your request. We may deny your request in certain cases, including if it is not in writing or if you do not give us a reason for the request.

Right to Receive an Accounting of Disclosures: You have the right to request an “accounting” of certain disclosures that we have made of PHI about you. This is a list of disclosures made by us during a specified period of up to 6 years, other than disclosures made: for treatment, payment, and health care operations; for use in or related to a facility directory; to family members or friends involved in your care; to you directly; pursuant to an authorization by you or your personal representative; for certain notification purposes (including national security, intelligence, correctional, and law enforcement purposes); as incidental disclosures that occur as a result of otherwise permitted disclosures; as part of a limited data set of information that does not directly identify you; and before April 14, 2003. If you wish to make such a request, please contact our Privacy Official identified on the last page of this Notice. The first list that you request in a 12-month period will be free, but we may charge you for our reasonable costs of providing additional lists in the same 12-month period. We will tell you about these costs, and you may choose to cancel your request at any time before costs are incurred.

Right to a Paper Copy of this Notice: You have a right to receive a paper copy of this Notice at any time. You are entitled to a paper copy of this Notice even if you have previously agreed to receive this Notice electronically. To obtain a paper copy of this Notice, please contact our Privacy Official listed in this Notice.

IV. COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with us or the Secretary of the United States Department of Health and Human Services. To file a complaint with our office, please contact our Privacy Official at the address and number listed below. We will not retaliate or take action against you for filing a complaint.

V. QUESTIONS

If you have any questions about this Notice, please contact our Privacy Official at the address and telephone number listed below.

VI. PRIVACY OFFICIAL CONTACT INFORMATION

You may contact our Privacy Official at the following address and phone number:

Privacy Official: Lenora Kinney, 302 Oddville Avenue, Cynthiana, KY 41031 (859) 234-8750.

VII. Red Flags Rule:

The Wedco District Health Department, and all its agents, employees and subcontractors, shall adhere to and comply with any and all applicable requirements of Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681m (e)); the administrative regulations promulgated thereto, including but not limited to 16 C.F.R. Part 681 (the “Red Flags Rule”); and any written identity theft prevention program developed and implemented by the Local Health Department and/or the Kentucky Department for Public Health. Additionally, any Contractor shall indemnify and hold harmless the Local Health Department, the Kentucky Department for Public Health, and their agents, representatives, officers, directors, employees, insurers, successors, and assigns from and against any and all expenses, costs (including attorneys’ fees), causes of action, liability, loss and/or damages suffered or incurred by any of them, that results from or arises out of any acts, errors, or omissions of the Contractor, or its agents, employees, or subcontractors, that violate Section 114 of the Fair and Accurate Credit Transactions Act of 2003; any administrative regulations promulgated thereto, including but not limited to the Red Flags Rule; or any written identity theft prevention program developed and implemented by the Local Health Department or the Kentucky Department for Public Health.

Wedco Red Flag Rule Policy:

POLICY: Wedco District Health Department, (the “Agency”) will comply with the “Red Flag” Rule of the Fair and Accurate Credit Transactions Act of 2003 (“FACT”) in order to help ensure that the Agency identifies, detects, prevents, and mitigates incidences of identity theft. The Agency Senior Management or a committee of the Agency Senior Management is responsible for compliance with this Policy.

PROCEDURE:

The Agency will identify and detect “red flags” in order to help prevent possible incidences of identity theft. “Identity theft” means a fraud committed or attempted using the identifying information of another person without authority. “Red flags” are patterns, practices, or specific activities that may indicate identity theft. Possible “red flags” identified by the Agency and action to be taken by the Agency includes:

- Alerts, notifications, or other warnings received from payors, regulators, enforcers, etc. involved in fraud detection.

- Presentation of suspicious documents: For our Home Health patients, specifically during the admission process, staff will ask each patient/client for photo identification. Staff will compare pictures of patients/clients with the physical characteristics of patients/clients, and document and attempt to resolve any discrepancies. When patients/clients are unable to present identification that includes a photo, staff will document the reason that no picture identification was obtained. In our clinic setting, we will supply a patient who is lacking proper identification to identify them, a form that requires a Notary signature that will verify that the individual is who they claim to be. In addition, we will take a digital photograph of the person. Then we can scan the form in to the PC and apply the photo to the form. This can be kept in the persons chart to positively identify them. We would need to repeat the process with the person every five years to keep up with potential changes in their appearance over this time period.

- When discrepancies are identified or identification that includes pictures cannot be obtained, staff will notify their supervisors and document that they have done so.

- Presentation of suspicious personal identifying information, including first name or first initial and last name, in combination with the following:
 - Social Security Number, Driver's license number, Account number, credit card number, or debit card number in combination with any security code, access code, or password that would allow access to a financial account of the patient/client, Tribal identification card, Federal or state identification cards.

 - Notice from patients/clients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Agency's accounts.

- 1. Discrepancies in patients'/clients' medical records, including treatment or services that are inconsistent with their history, physical, and/or diagnosis.
 - Complaints or questions from patients/clients about:
 - Bills for another individual, bills for products or services not received, bills from providers/suppliers from whom services were not received, Explanation of Benefits for services or items that patients/clients did not receive.

1. The Agency will attempt to prevent and/or mitigate identity theft using the following mechanisms:

- Monitoring accounts for evidence of identity theft, contacting patients/clients, changing passwords, security codes, or other security devices that permit access to patient/client information, notifying law enforcement, determining that no response is warranted under the circumstances.
- The Agency Senior Management of the Agency is responsible for implementation of this Policy. The Agency Senior Management will approve this Policy, review reports prepared by staff regarding compliance with this Policy and will approve significant changes to this Policy as necessary to address changing identify theft risks.
- The Agency will provide initial training regarding the requirements of this Policy to staff, including at a minimum staff responsible for admission of patients/clients. After initial training has been provided, the Agency will provide additional training periodically as needed.
- The Agency will ensure that subcontractors who provide services to its patients/clients on its behalf also comply with the requirements of the “Red Flag Rule.” Specifically, Agency will include language in all contracts/agreements with its subcontractors requiring subcontractors to comply with the “Red Flag Rule.”

This Policy shall be periodically updated by the Agency Senior Management to reflect changes in identity theft risks and new methods for “red flag” detection, prevention, and mitigation.