NOTICE OF PRIVACY PRACTICES

Your Rights

When it comes to your health information, you have certain rights. You have the right to:

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say “no” to your request, but we’ll tell you why in writing within 60 days.

Request Confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say “yes” to all reasonable requests.

Ask us to limit what we use or share

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say “no” if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say “yes” unless a law requires us to share that information.

Get a list of those with whom we’ve shared information

- You can ask for a list (accounting) of the times we’ve shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We’ll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice

- A copy of this notice is provided within your admission packet at the time of admission; should you be unable to locate the notice please feel free to ask for another copy.

Effective Date February 01, 2014

NOTICE OF PRIVACY PRACTICES

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated

- You can complain if you feel we have violated your rights by contacting us directly at the facility, or by calling the Compliance Hotline at 1-800-320-4798. Calls to the Hotline are anonymous, unless you choose to give your name.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints/.**
- You may also file a complaint with:

  Office Of The Secretary
  1901 N. Du Pont Highway, Main Bldg.
  New Castle, DE 19720
  (302) 255-9040; (302) 744-4556
  FAX: (302) 255-4429

  Division Of Developmental Disabilities Services
  (302) 744-9600; FAX: (302) 744-9600
  Woodbrook Professional Center
  1056 South Governor's Avenue, Suite 101
  Dover, DE 19904
  Stockley Center - (302) 934-8031

  Division Of Long Term Care Residents Protection
  3 Mill Road, Suite #308
  Wilmington, DE 19806
  (302) 577-6661; FAX: (302)577-6672

- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care

- Share information in a disaster relief situation
- Include your information in a facility directory

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:

- We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures

The facility is required to maintain a record of all disclosures of information contained in the medical record to a third party, including the purpose of the disclosure. We typically use or share your health information in the following ways:

To treat you

We can use your health information and share it with other professionals who are treating you.
Example: A doctor treating you for an injury asks another doctor about your overall health condition.

To run our organization

We can use and share your health information to run our practice, improve your care, and contact you when necessary.
Example: We use health information about you to manage your treatment and services.

To bill for your services

We can use and share your health information to bill and get payment from health plans or other entities.
Example: We give information about you to your health insurance plan so it will pay for your services.

NOTICE OF PRIVACY PRACTICES

How else can we use or share your health information?

We are allowed, or required, to share your information in other ways – usually in ways that contribute to the public good, such as public health and research.

Help with public health and safety issues

We can share health information about you for certain situations such as:

- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Do research

We can use or share your information for health research.

Comply with the law

We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

Respond to organ and tissue donation requests

We can share health information about you with organ procurement organizations.

Work with a medical examiner or funeral director

We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests

We can use or share health information about you:

- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions

We can share health information about you in response to a court or administrative order, or in response to a subpoena.

Effective Date February 01, 2014

NOTICE OF PRIVACY PRACTICES

We have to meet many conditions in the law before we can share your information for these purposes. For more information you can visit: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html**.**

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.
- We never sell or market personal information
- We will make available copies of reports and records related to a person's examination or treatment, in a timely manner, upon your request or that of your legal representative.
- When a patient's psychiatric, psychological, or psych-therapeutic records are requested by the patient or the patient's legal representative, the facility may provide a report of examination and treatment in lieu of copies of records. Upon a patient's, or their legal representative's, written request, complete copies of the patient's psychiatric records must be provided directly to a subsequent treating psychiatrist.
- We will allow you to examine original records in our possession under reasonable terms to assure that the record will not be damaged, destroyed or altered.

The State of Delaware:

- Recognizes the psychotherapist-patient privilege
- Recognizes the physician-patient privilege
- Maintains cancer registries
- Genetic testing statutes are available and provide a cause of action for violations of provisions
- Holds that HIV/AIDS records are privileged and provides cause of action
- Holds that mental health records of an individual are confidential and may not be disclosed without the patient's authorization. However, does NOT provide a civil or criminal remedy for the release or public disclosure of mental health information.
- Has legislation requiring notification of security breaches involving personal information.

Effective Date February 01, 2014

NOTICE OF PRIVACY PRACTICES

For more information you can visit:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

New Castle
Health & Rehabilitation Center
A NOT FOR PROFIT FACILITY

Privacy Official: Administrator

Telephone Number: 302-328-2580

Email Address: Administrator@newcastle-health.com

Delaware, DE

HIPAA FAQs

Q. What does the HIPAA Privacy Rule do?

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data –for example, to protect public health.
  For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.
- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

NOTICE OF PRIVACY PRACTICES

Q. Can a doctor, laboratory, or other health care provider share patient health information for treatment purposes by fax, e-mail, or over the phone?

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

- A laboratory may fax, or communicate over the phone, a patient's medical test results to a physician.
- A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient.
- A hospital may fax a patient's health care instructions to a nursing home to which the patient is to be transferred.
- A doctor may discuss a patient's condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient's treatment regimen with a nurse who will be involved in the patient's care.
- A physician may consult with another physician by e-mail about a patient's condition.
- A hospital may share an organ donor's medical information with another hospital treating the organ recipient.

The Privacy Rule requires Public Health to apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve confirming the fax number with the intended recipient. Similarly, you may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his/her voice.

Q. What is ePHI?

It is an acronym for electronic protected health information. Electronic Protected Health Information (ePHI) is either transmitted by electronic media or maintained in electronic media.

Q. What is PHI?

It is an acronym for protected health information. Protected Health Information is personal and sensitive medical information related to an individual's health care.

NOTICE OF PRIVACY PRACTICES

Q. Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

No. All States have laws that require providers to report cases of specific diseases to public health officials. The HIPAA Privacy Rule permits disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing protected health information with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births, investigating the occurrence and cause of injury and disease, and monitoring adverse outcomes related to food (including dietary supplements), drugs, biological products, and medical devices. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Q. Can you leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready?

Yes. The HIPAA Privacy Rule permits Public Health to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit Public Health from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, you should take care to limit the amount of information disclosed on the answering machine. For example, you might want to consider leaving only your name and number and other information necessary to confirm an appointment, or ask the individual to call back.

You may also leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits Public Health to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, you need to use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

In situations where a patient has requested that you communicate with him in a confidential manner, such as by alternative means or at an alternative location, you must accommodate that request, if reasonable.

Q. What does the HIPAA Security Rule mean by physical safeguards?

The Security Rule requires Public Health to implement physical safeguard standards for our electronic information systems. The Division of Public is now required to implement policies and procedures to protect all information systems including our facilities that store electronic protected health information, from natural and environmental hazards, and unauthorized intrusion. DPH standards include facility access controls, workstation use, workstation security, and device and media controls.

Q. What if certain state laws are different from HIPAA?

If a state law is more restrictive than HIPAA, then the state law prevails. Otherwise, if state law contradicts HIPAA, you must follow HIPAA.

Q. Who do I need to have business associate agreements with?

You must have business associate agreements with any entity that performs a business function for you and that you share PHI with. This can include software vendors, medical reviewers, lawyers, auditors, a clearinghouse or payers. Any of these would be considered business associates.

Q. Under HIPAA, can we still report vital health statistics such as births and deaths?

Yes, you can report vital health statistics if your state or local law requires such reporting and you report this information to a public health authority authorized by law to collect or receive it.

You do not need prior authorization to report this information to a public health authority. However, you must get consent before you report this information to newspapers or other media outlets.

Q. Can health care providers engage in confidential conversations with other providers or with patients/clients, even if there is a possibility that they could be overheard?

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients/clients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Covered

entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient/client, a provider or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient/client over the pharmacy counter or with a physician or the patient/client over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective and high quality health care.

Q. What is encryption?

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Q. Does the HIPAA Security Rule allow for sending electronic PHI in an email or over the Internet? If so, what protections must be applied?

The HIPAA Security Rule does not expressly prohibit the use of email for sending electronic protected health information (ePHI). However, the standards for access control, integrity, and transmission security require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to ePHI. The standard for transmission security also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect ePHI as it is transmitted, select a solution, and document

the decision. The Security Rule allows for ePHI to be sent over an electronic open network as long as it is adequately protected.

Q. Does the HIPAA Security Rule apply to written and oral communications?

No. The Security Rule is specific to electronic protected health information (ePHI). It should be noted however that ePHI also includes telephone voice response and faxback systems because they are used as input and output devices for computers. EPHI does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. HIPAA Privacy Rule addresses all mediums of PHI, including written and oral. Information on the Privacy Rule can be found online at: http://www.hhs.gov/ocr/hipaa.

Q. What are our duties when we receive a subpoena for medical records or other protected health information?

When you receive a subpoena for protected health information, it is necessary to determine whether the subpoena was issued pursuant to a judicial or administrative order.

When the subpoena is issued through or pursuant to a court or administrative tribunal order, you may disclose the requested information without authorization. Note that a covered entity may disclose; it does not have to disclose.

Go to Section 164.512(e) Disclosures for Judicial and Administrative Proceedings for more information.

Q. Do we need authorization prior to disclosing information regarding the location of a patient?

If the patient is present and has the capacity to make healthcare decisions, you may use or disclose the patient's PHI if you

- obtain the individual's agreement (either orally or in writing)
- provide the individual with the opportunity to object to the disclosure, and the individual does not express an objection
- reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure

Go to Section 164.510(b) Uses and Disclosures for Involvement in the Individual's Care and Notification Purposesfor more information.

NOTICE OF PRIVACY PRACTICES

Q. Is an authorization required by anyone before we make a disclosure about child abuse?

No authorization is required as long as the information is disclosed to a public health authority or other appropriate government agency authorized by law to receive reports of child abuse or neglect.

The regulations define a "public health authority" as

- an agency or authority of the United States
- a state, a territory, a political subdivision of a state or territory
- an Indian tribe
- a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate

Go to Section 164.512(b) Uses and Disclosures for Public Health Activities for more information.

Q. How often must we give the same patient an NPP?

Direct treatment providers that are covered entities (CEs) are only required to give out their privacy notices one time to each patient, assuming that the privacy notice contains a statement reserving the right to make changes.

You must post your privacy notice prominently in your facility. If you change the notice, you must update the posted notice and all copies and make sure each shows the effective date. Keep in mind that you must update the notice and make it available prior to the change taking effect.

Q. Must an Authorization include an expiration date?

The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire "one year from the date the Authorization is signed", "upon the minor's age of majority" or "upon termination of enrollment in the health plan". An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event. The fact that the expiration date on an Authorization may exceed a time period established by State law does not invalidate the Authorization under the Privacy Rule, but a more restrictive State law would control how long the Authorization is effective.

Q. Can an individual revoke his or her Authorization?

Yes. The Privacy Rule gives individuals the right to revoke, at any time, an Authorization they have given. The revocation must be in writing, and is not effective until the covered entity receives it. In addition, a written revocation is not effective with respect to actions a covered entity took in reliance on a valid Authorization, or where the Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

The Privacy Rule requires that the Authorization must clearly state the individual's right to revoke; and the process for revocation must either be set forth clearly on the Authorization itself, or if the covered entity creates the Authorization, and its Notice of Privacy Practices contains a clear description of the revocation process, the Authorization can refer to the Notice of Privacy Practices. Authorization forms created by or submitted through a third party should not imply that revocation is effective when the third party receives it, since the revocation is not effective until a covered entity which had previously been authorized to make the disclosure receives it.

Q. Does the HIPAA Privacy Rule provide rights for children to be treated without parental consent?

No. The Privacy Rule does not address consent to treatment, nor does it preempt or change State or other laws that address consent to treatment. The Rule addresses access to, and disclosure of, health information, not the underlying treatment.

Q. Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are:

1. When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law;
2. When the minor obtains care at the direction of a court or a person appointed by the court; and
3. When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases, the licensed health care provider may exercise his or her

professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.
