PARC
Partner. Achieve. Reach. Connect.
Exceptional Opportunities for People with Disabilities

What does HIPAA do?

HIPAA establishes:

- National uniform Electronic Transaction Standards (Electronic Data Interchanges) which requires health plans, health plans clearing houses and health plan providers who transmit data electronically to use and accept standard formats and standard medical code sets.
- Unique identifiers for providers, health plans, employers and individuals.
- Protections for the privacy of individually identifiable health information.
- Protections for the security of individually identifiable health information.

Violation Categories &Penalties for Non-Compliance:

- Violation Category
  - Did Not Know
  - Reasonable Cause
  - Willful Neglect - Corrected

Willful Neglect - Not Corrected **Civil Violation Category**	**Each Violation**	**All such Violations of an identical provision in a calendar year.**
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect - Not Corrected	$50,000	$1,500,000

Criminal Violation Category	**Potential Jail sentence in addition to possible Civil Penalty above**
Unknowingly or with Reasonable Cause	Up to 1 year
Under False Pretenses	Up to 5 Years
For Personal gain or malicious reasons	Up to 10 years

What is HIPAA?

HIPAA stands for the federal law entitled the Health Insurance Portability and Accountability Act, which was passed in 1996. Regulations issued under HIPAA that protect the privacy of health information for all Americans went into effect April 14, 2003.

How does HIPAA affect professionals in the MR/DD field?

As employees, contractors or volunteers in the MR/DD field, we are legally responsible to protect the health information of the people we serve. Special laws mandate the ways in which we store and share this information. All the individuals that we work with need to be given a privacy statement, which explains how their health information will be used, and their rights under HIPAA.

What information does HIPAA protect?

The HIPAA regulations safeguard Protected Health Information [PHI].

PHI includes an individual's:

- Health (Diagnosis)
- Provision of Care (Services Received)
- Payment of Services (How payment will be made)
- Information which identifies the individual (Name, address, social security, etc)

When can PHI be shared?

PHI may be shared for:

- Treatment (residential services, clinic, etc)
- Payment (billing of services)
- Health Care Operations (such as quality assurance, program oversight)

In most instances you do not need the individual's consent for these purposes unless you are sharing sensitive information (HIV/AIDS information, mental health records, etc) that is protected by special state laws.

When sharing information, how much information may I share?

For the purpose of payment and health care operations only the minimum information necessary must be shared. For purposes of treatment, the concept of minimum necessary should not impede the free flow of information necessary to ensure comprehensive treatment.

When do I need a special consent to share PHI?

Under most other circumstances, it would be necessary to get the consent of the individual and his or her representative to release their PHI. (For example: marketing, publicity, referrals, when requested for personal use/for personal records,etc.) In these cases, it is very important to explain carefully to the individuals that we serve what they are agreeing to and to use the agency's standard authorization form.

Are there other circumstances where information may be disclosed without consent?

There are a number of possible situations where this information can be disclosed for "public need" purposes without consent. These included, but are not limited to the following:

- Government audits and investigations
- Public health and safety
- A subpoena from the courts

What are the steps employees, contractors and volunteers need to take to protect the individual's PHI?

- Discussion - Do not discuss information in a public place where others can overhear; this includes discussing PHI in front of participants.
- Files - Make sure files are not kept where unauthorized people can see them and that they are locked away when not in use. Do not remove files from the building without prior authorization from appropriate administration. If you have been authorized to transport or have a file in your possession, you are responsible for ensuring that the file is secure (i.e.; do not leave the file in your unlocked car). Fax - When sending a fax, make sure an authorized person is on the other end to receive it unless you have confirmed that the fax machine is in a secure setting. Check the fax number to make sure it is correct. Always use a fax cover sheet and include standard confidentiality notices,
- Computers - All computers must be password protected. Never share your computer password with anyone. Your computer screen should face away from the public viewing area. When stepping away from a computer in use, you can protect information by closing all applications and using a screen saver. Do not send PHI by e-mail unless it is encrypted.
- Printer/copier - When printing to a "common area" printer such as the Kyocera's please use the secure printing option to ensure you are at the printer when the print out is generated. Please also be sure when printing or making copies you do not leave anything on the printer.

How do I dispose of documents containing PHI?

Anything containing PHI must be disposed of in a way that makes the information unreadable, such as a shredder.

If I am asked to give out information, what should I do?

Let the person asking you for information know that PARC has a HIPAA policy that requires all requests for information to be in writing on a PARC authorization form, and that the request must be reviewed by the Director of Quality Assurance before any information or documents can be copied or released.

Provide the person with the proper form.

Let the person asking for information know that PARC will respond to all written requests and will release all appropriate information and documents after the form has been reviewed and the appropriate documents have been copied.

If the person has any questions or concerns, please direct them to Kim Spielberg, Director of Quality Assurance and Compliance, XT 2252.

Please note that HIPAA also applies if people call you for information. In the event that an attorney or a reporter contacts you for information, all of the same rules apply. Be cordial, but immediately direct all attorney inquiries to General Counsel and all reporter or media inquiries to the Director of Development. Absolutely no information must be released. Simply inform them that we have privacy policies in place and information cannot be released without proper consent.

PARC AGENCY POLICY

DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR TREATMENT, PAYMENT & HEALTH CARE OPERATIONS

SCOPE OF POLICY

This policy applies to all agency staff members, and all volunteers, consultants, interns, contractors and subcontractors at the agency [collectively referred to herein as "Agency Staff"].

STATEMENT OF POLICY

PARC is committed to protecting the privacy and confidentiality of health information relating to the people we serve. Protected health information (as defined below AND in the agency's policy on Disclosures of Protected Health Information For Treatment, Payment and Health Care Operations), is strictly confidential and must never be givenout, released, or confirmed to anyone who is not authorized under the agency's policies or applicable law to receive such information.

IMPLEMENTATION OF POLICY

A. PROTECTED HEALTH INFORMATION [PHI]

For purposes of this policy, the term "Protected Health Information" [PHI] means any individual information (including very basic information such as a participant's name or address) that:[1]

1. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

2. Either identifies the individual or could reasonably be used to identify the individual (e.g. initials, Medicaid #, etc.).

Some examples of PHI are any information about:

- The individual's health condition (such as the condition the individual may haveor a diagnosis)
- Health care services the individual has received or may receive in the future (such as PT or OT)
- The individual's health care benefits under an insurance plan (such as whether a prescription is covered)
- Whether an individual is receiving health care services from our agency or any other health care provider

When combined with:

- Demographic information (name, address, race, gender, ethnicity, marital status)
- Geographic information (home or work address)
- Unique numbers that may identify the individual (social security number, medical record number, telephone number, driver's license number)
- Other types of information that may identify the individual

This policy applies to PHI in any form, including spoken, written, or electronic.

It is the responsibility of every Agency Staff memberto preserve the privacy and confidentiality of all PHI and to ensure that PHI is used and disclosed only as permitted under the agency's policies and applicable law. This includes, but is not limited to, compliance with the protective procedures below.

B. USES AND DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS [TPO]

Unless PARC has received consent from the individual for, or applicable law otherwise requires or permits,[2] a particular use or disclosure of protected health information, PHI may only be used or disclosed for purposes of (i) our agency's treatment activities, payment activities, and health care operations, and (ii) certain treatment activities, payment activities, and health care operations of other health care providers and of health plans. Treatment, payment and health care operations are defined as follows:

TREATMENT:

For purposes of this policy, the term "treatment" means providing, coordinating or managing the individual's health care and any related services.[3] Some examples of treatment activities involving the use or disclosure of protected health information are:

- Using PHI about an individual's disease or condition to diagnose or provide care
- Disclosures of PHI to other health care providers who are involved in taking care of the individual
- Disclosures of PHI to another health care provider in order to obtain advice about how best to diagnose or provide care to the individual
- Disclosures of PHI to another health care provider to whom the individual has been referred to ensure that this health care provider has the necessary information to diagnose or provide care to the individual

PAYMENT:

For purposes of this policy, the term "payment" generally means the activities undertaken by the agency to obtain or provide reimbursement for the provision of health care.[4]Some (but not all) examples of payment activities involving the use or disclosure of protected health information are disclosing the individual's PHI to:

- A health insurance plan to determine whether it will provide coverage for the individual's treatment
- Obtain pre-approval before providing a treatment or service, such as admitting the individual to the agency for a particular type or surgery
- His or her health insurance plan to obtain reimbursement after the agency has treated the individual.

Uses and disclosures of PHI for the agency's payment purposes are subject to the HIPAA Privacy Regulations' "minimum necessary" standard. Please refer to the agency's policy on Minimum Necessary Standards for both Routine and Non Routine activities.

HEALTH CARE OPERATIONS:
For purposes of this policy, the term "health care operations" generally refers to those general business and administrative functions of the agency that are required in order to operate and perform its health care functions.[5] Some (but not all) examples of uses and disclosures of protected health information for health care operations are:

- For quality assurance and utilization review purposes
- For education and training of students and other trainees
- To recommend possible treatment options or alternatives, or health related benefits or services, that may be of interest to the individual
- For legal services, business planning, and other business management and general administrative activities
- To raise funds for the benefit of the agency

Uses and disclosures of PHI for the agency's health care operations are subject to the HIPAA Privacy Regulations' "minimum necessary" standard. Please refer to the agency's policy on Minimum Necessary Standards for both Routine and Non Routine activities.

DISCLOSURE FOR OTHER PROVIDER'S TREATMENT, PAYMENT OR HEALTHCARE OPERATIONS
Our agency also may disclose PHI to other providers for their treatment, payment and health care operations as follows:[6]

- For its treatment activities
- For its payment activities
- Our agency may disclose PHI to a health plan or another health care provider for its health care operations, **but only if:**
    - Both our agency and the other party have, or had, a relationship with the individual whose information is being disclosed;
    - The PHI being disclosed pertains to that current (or previous) relationship; and
    - The disclosure is for certain limited health care operations activities, including conducting quality assurance and/or quality improvement activities, education or training of students and other staff, reviewing the competence or qualifications, or the performance, of health care professionals, accreditation, licensing, credentialing, and fraud and abuse detection or compliance activities.

Disclosures of PHI for the others' payment activities or health care operations are subject to the HIPAA Privacy Regulations' "minimum necessary" standard. Please refer to the agency's policy on Minimum Necessary Standards for both Routine and Non Routine activities.

C. DE-IDENTIFIED INFORMATION NOT SUBJECT TO TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS RESTRICTED
PHI is considered "de-identified" when all elements that have the potential to identify the individual have been removed. PHI will be deemed de-identified when (i) a person with appropriate knowledge and experience in scientific and statistical principles for de-identifying information has determined that there is a very small risk that the information can be used to identify the individual and has documented the analysis that justifies that

decision or (ii) certain specific identifying elements regarding the individual and his or her relatives, employers and household members have been removed and the remaining information cannot be used to identify the individual.[7]
The elements that must be removed include the following:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes
- All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements, including year, indicative of such age, except that ages and elements may be aggregated into a single category of 90 or older
- Telephone numbers
- Fax numbers
- Electronic mail (e-mail) addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers; including license plate numbers
- Device identifiers and serial numbers
- World wide web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers; including finger and voice prints
- Full face photographic images and comparable images
- Any other unique identifying number, characteristic or code

Because de-identified information is no longer considered PHI, such de-identified information is not subject to the Treatment, Payment and Health Care Operations restriction and generally may be used and disclosed without limitation. However, Agency Staff must obtain approval from the Chief Privacy Officer, or designee that protected health information has been appropriately de-identified prior to treating such information as de-identified.

D. USES OF PHI FOR REASONS OTHER THAN TREATMENT, PAYMENTS AND HEALTH CARE OPERATIONS

Agency Staff are instructed to consult their department supervisors if they are unsure whether a particular use or disclosure satisfies the definition of Treatment, Payment or Health Care Operations, or if they believe they need to use or disclose PHI for reasons other than TPO and they are unsure whether an exception applies or if the agency has obtained an authorization for that particular use or disclosure. Department supervisors will be responsible for providing guidance or directing the individual to a Deputy Privacy Officer or the Chief Privacy Officer.

Violations:
The agency's Chief Privacy Officer has general responsibility for implementation of this policy. Members of our Agency Staff who violate this policy will be subject to disciplinary action, as outlined in the employee handbook and further defined by appropriate laws and regulations, up to and including termination of employment or contract with PARC. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the agency's Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, PARC will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action, as outlined in the employee handbook and further defined by appropriate laws and regulations, up to and including termination of employment or contract with PARC.

QUESTIONS:
If you have questions about this policy, please immediatelycontact your department supervisor or Deputy Privacy Officer, or if not available, the agency's HIPAA Security Officer or Chief Privacy Officer. It is important that all questions be resolved as soon as possible to ensure PHI is used and disclosed appropriately.

Effective Date: May 19, 2003

Updated: July 2013

[1] 45 CFR §164.501

[2] 45 CFR §64.50(c) (1) -(c) (4)

[3] 45 CFR §64.501

[4] 45 CFR §64.501

[5] 45 CFR §64.501

[6] 45 CFR §164.506 (c) (4)

[7] 45 CFR §164.514 (b)

PARC AGENCY POLICY

STAFF CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

SCOPE OF POLICY

This policy applies to all agency staff members, and all volunteers, consultants, interns, contractors and subcontractors at the agency.

STATEMENT OF POLICY

PARC is committed to protecting the privacy and confidentiality of health information about the people we serve. Protected health information (as defined below AND in the agency's policy on Disclosures of Protected Health Information For Treatment, Payment and Health Care Operations), is strictly confidential and should never be given, nor confirmed to anyone who is not authorized under the agency's policies or applicable law to receive this information.

IMPLEMENTATION OF POLICY

A. DEFINITION OF PROTECTED HEALTH INFORMATION [PHI]

For purposes of this policy, the term "protected health information" means any individual information (including very basic information such as a participant's name or address) that:

1. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

2. Either identifies the individual or could reasonably be used to identify the individual (e.g. initials, Medicaid #, etc.).

Please see the agency's policy on Disclosures of Protected Health Information for Treatment, Payment and Health Care Operations for examples of protected health information.

This policy applies to PHI in any form, including spoken, written or electronic form. It is the responsibility of every Agency Staff to protect the privacy and preserve the confidentiality of all PHI and to ensure that PHI is used and disclosed only as permitted under the agency's policies and applicable law. This includes, but is not limited to, compliance with the protective procedures below.

B. PUBLIC VIEWING/HEARING

Agency Staff must keep PHI out of public viewing and hearing range. For example, PHI must not be left in conference rooms, out on desks, or on counters or other areas where the information may be accessible to the public or to other employees or individuals who do not have a need to know the PHI. Agency Staff must also refrain from discussing PHI in public areas (examples of public areas include, but are not limited to, lunchrooms, reception areas, hallways, etc), unless doing so is necessary to provide treatment. Agency Staff must also take care in sharing PHI with families and friends of the people we serve. Such information may generally only be shared with an individual's "personal representative" or to an individual's family member, relative or close personal friend who is involved in the care or

payment for care. Even in the latter circumstance, information cannot be disclosed unless the individual has had a chance to agree or object to the disclosure, and you may only disclose information that is relevant to the involvement of that family member, relative or close personal friend in the individual's care or payment for the individual's care, as the case may be.

C. DATABASES AND WORKSTATIONS

Agency Staff must ensure that they exit any confidential database upon leaving their work stations so that PHI is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Agency Staff must not disclose or release to other persons any item or process which is used to verify their authority to access or amend PHI, including but not limited to, any password, personal identification number, token or access card, or electronic signature. Each Agency Staff member will be liable for all activity occurring under his or her account, password and/or electronic signature. These activities may be monitored.

D. DOWNLOADING, COPYING OR REMOVING

Agency Staff must not download, copy or remove from the agency any PHI, except as necessary to perform their duties at the agency. Upon termination of employment or contract with the agency, or upon termination of authorization to access PHI, Agency Staff members must return to the agency any and all copies of PHI in their possession or under their control.

E. EMAILING AND FAXING INFORMATION

Agency Staff must not transmit protected health information over the Internet (including email) and other unsecured networks unless using a secure encryption procedure. Transmission of PHI is permitted by fax only if the Agency Staff member sending the information ensures that the intended recipient or designee is available to receive the fax as it arrives, or confirms that there is a dedicated fax machine that is monitored for transmission of sensitive information. Agency Staff must use fax cover sheets that include standard confidentiality notices, and should request that the recipient call the staff member upon receipt of the fax.

VIOLATIONS

The agency's Chief Privacy Officer has general responsibility for implementation of this policy. Members of our Agency Staff who violate this policy will be subject to disciplinary action, as outlined in the employee handbook and further defined by appropriate laws and regulations, up to and including termination of employment or contract with PARC. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the agency's Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, PARC will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action, as outlined in the employee handbook and further defined by appropriate laws and regulations, up to and including termination of employment or contract with PARC.

QUESTIONS

If you have questions about this policy, please contact your department supervisor or Deputy Privacy Officer, or if not available, the agency's HIPAA Security Officer or Chief Privacy Officer, immediately. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.

Effective Date: May 19, 2003

Updated: July 2013