Health Insurance Portability and Accountability Act (HIPAA)

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996, (HIPAA), is the first comprehensive Federal law that provides consumers with privacy and security protection of their health information and their right to restrict the use and disclosure of this information. The privacy legislation was effective April 14, 2003. The security legislation is effective April 21, 2005. All organizations involved in providing health care services must comply with the privacy and security laws including health insurance companies, doctor's offices, pharmacies, hospitals, nursing homes, home care agencies, and any other locations that provide health care services.

What are some Examples of HIPAA violations?

- A celebrity was in the Medical Facility and you tried to sneak a peek at the paper or electronic record.
- You discussed patient information on an elevator, in a lobby, cafeteria, or other public locations, or to individuals not involved in the patient's care.
- One of your family members, neighbors, or friends is a patient and you kept others up to date on the events of his/her case.

What Can You Do?

Be mindful of ways to protect patient confidentiality and patient information, such as:

- Close patient room doors when discussing treatment plans
- Close curtains and speak very softly when in a semi-private room
- Never discuss patients or treatment in public areas (e.g. elevators, cafeteria)
- Never leave messages regarding patient conditions or test results on answering machines or with anyone other than the patient
- Never call/page patients in such a way as to reveal their health issues (e.g. "Patient Smith, please return to the dialysis unit")
- Never leave health information unattended in an area where others may inappropriately see and/or remove it
- Never leave a computer without signing off
- Never allow another person to use your computer after using your sign-on.
- Never share computer passwords with anyone
- Position computer screen so that visitors or people walking by cannot view information
- Require that a patient sign an Authorization to Release medical information form before provider copies of their health information. Requests for copies of records require a signed authorization placed in the patient record unless the record is needed for treatment by another healthcare provider. All legal requests for

medical records (attorneys and subpoenas) should be referred to the Office of HIPAA Compliance.

Notice of Privacy Practices

Every patient treated must receive a written Notice of Privacy Practices. The notice is available in the Privacy Office and in every area where patients are registered to receive care. In the Notice of Privacy Practice, patients are advised of their rights. Some of these rights include the following:

- Receive a written notice of how Medical Facility uses their information including treatment, payment, and healthcare operations (e.g., quality assurance and patient satisfaction)
- Receive a copy of their health information
- Amend their health information
- Be informed of all recipients of their health information
- Restrict the use of their health information
- Request how their health information is used
- Complain about perceived violations of privacy

HIPAA Security

What is our Security Goal?

As mandated by HIPAA, our goal is to ensure confidentiality, integrity, and availability of all Electronic Patient Health Information (ePHI) so that it is not sabotaged, attacked, lost, stolen or misused.

What is ePHI?

Electronic Patient Health Information that can be linked to a specific individual's identity, medical condition, treatment or status as a patient.

How Can Security Fail?

Intentional "attack" (external – hacker or internal - employee)

- Malicious software (i.e. Virus, worm, Trojan-horse)
- Password stolen or code broken
- Imposter calling/e-mailing/instant messaging and asking for protected information
- USB drive / jump drive, or laptop stolen
- Employees accessing records they have no legitimate need to see

Employee carelessness

- Leaving your computer logged on, accessible and unattended
- Letting others know your password
- Downloading games or other unauthorized software
- Using instant messaging or chat rooms
- Misdirected e-mail/faxes

Whether it is an intentional attack or employee carelessness, the negative impact on the system is the same.

Faxing

Employees should take reasonable steps to ensure that fax transmissions are sent to and received by the intended recipient including:

- Ensuring that fax machines that receive confidential information are in a secure area
- Confirm intended recipient fax machine number or pre-program frequent recipients of confidential information
- Use ‘confirm” receipt to verify that all faxed information was received by intended recipient

Electronic Mail (E-Mail)

- Confidential information may not be transmitted via electronic mail unencrypted unless there are no reasonable available alternatives for transmission
- Confidential information (including patient name or medical record number) may not appear in the header (subject line) of an e-mail message
- Subject line must make reference to the fact that the message contains confidential information
- HIV/AIDS, Mental Health or Substance Abuse patient information can never be included in an e-Mail

Action Steps to Take Every Day/Daily Reminders

Don't:

- Give anyone your password, ever, for any reason
- Download any software without first checking with IT
- Open any unknown web site or e-mail attachment
- Send patient information in e-mails going outside the network or in instant messages of any kind
- Leave your workstation without logging off your computer
- Give out patient data without proper authorization

Do:

- Choose a strong password (8 characters or longer, mix sets of characters) and change it when prompted
- Follow computer prompts to update virus scans when they appear on your computer screen
- Proof addresses when sending patient information
- Maintain heightened vigilance
- Follow all approved information security procedures
- Report anything that looks unusual

HIPAA regulations require that healthcare organizations have policies and procedures in place to protect patient's privacy and security. These policies stipulate how Medical Facility staff can use, disclose and dispose of health information.

Compliance with HIPAA regulations is a law but it is also an expectation of all employees including temporary employees.

HIPAA Orientation Acknowledgement

Please Remember…

- Be HIPAA Aware
- Think Patient Confidentiality
- Secure your own area
- Ask questions such as “Why do I need this information?”
- Help Educate Others

I will be responsible for my misuse, wrongful disclosure, and unauthorized access of confidential information. I understand that my failure to comply with the content of this document may result in the termination of my assignment including civil and legal liability.

By: Temporary Associate	By: Vendor Partner Name
_____	_____
Signature	Signature
_____	_____
Print Name	Print Name
_____	_____
Date	Date