HIPAA: Security & Privacy Compliance

As a healthcare worker, you are part of the "healthcare provider" network and therefore are required to comply with HIPAA rules and regulations regarding Protected Health Information (PHI). Workers in dietary, engineering, housekeeping, etc. may have access to PHI and also are required to comply with HIPAA regulations.

The HIPAA Privacy & Security Rules were developed by the Department of Health and Human Services and protects our fundamental right to privacy and confidentiality of personal medical information that is shared with doctors, hospitals, and others. It is part of the Health Insurance Portability and Accountability Act (HIPAA) enacted by Congress.

Basically, the Privacy Rule does the following:

- Imposes restrictions on the use and disclosure of personal health information
- Gives patients greater access to their medical records
- Gives patients greater protection of their medical records

The Security rule protects:

- The confidentiality of protected health information (PHI) that is shared or disclosed in electronic form
- The integrity of the electronic information (Electronic PHI cannot be changed or deleted once it is created)
- Accessibility of PHI – only authorized personnel would be allowed to access the information

PROTECTED HEALTH INFORMATION (PHI)

When a patient gives personal health information to a covered entity, that information becomes Protected Health Information – or PHI.

PHI includes any information – oral, recorded, on paper, or sent electronically – about a person's physical or mental health, services rendered or payment for those services, and that includes personal information connecting the patient to the records.

Examples of information that might connect personal health information to the individual include:

- The individual's name or address
- Social security or other identification numbers
- Physician's personal notes
- Billing information
- Verbal discussions between healthcare workers about a patient, medical condition, planned treatment and plan of care

THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

HIPAA's Privacy Rule is all about the use and disclosure of PHI. With few exceptions, PHI can't be used or disclosed by anyone unless it is permitted or required by the Privacy Rule.

PHI is used when a healthcare worker is viewing a medical record or examining testing or results.

PHI is disclosed when a healthcare worker is releasing or sharing private patient information including emailing, faxing, or discussing the information verbally.

You are ONLY permitted to use or disclose PHI:

- For treatment, payment, and healthcare operations.
- With authorization or agreement from the individual patient.
- For disclosure to the individual patient.
- For incidental uses such as physicians talking to patients in a semi-private room.

You are required to release PHI for use and disclosure:

- When requested or authorized by the individual – although some exceptions apply.
- When required by the Department of Health and Human Services (HHS) for compliance or investigation.

REQUIRED WRITTEN AUTHORIZATION

The final ruling makes consent for routine healthcare optional. But you are required to get a signed authorization from the patient if you use or disclose his or her PHI for purposes other than:

- Treatment.
- Payment.
- Healthcare operations.

Generally, authorization is required to use PHI:

- For use or disclosure of psychotherapy notes.
- For disclosure to an insurer or employer.
- For research purposes, unless a documented waiver is obtained from the Institutional Review Board (IRB) or a privacy board.
- For use and disclosure to third parties for marketing activities such as promoting services or selling lists of patients.

However, covered entities may communicate freely with patients about treatment options and health-related information.

THE MINIMUM NECESSARY REQUIREMENT

In general, use/disclosure of PHI is limited to the minimum amount of health information necessary to get the job done right. That means:

- Covered entities must develop policies and practices to make sure the least amount of health information is shared.
- Employees must be identified who regularly access PHI along with the types of PHI needed and the conditions for access.

The Minimum Necessary requirement does not apply to use/disclosure of medical records for treatment, since healthcare providers need the entire record to provide quality care. But it does apply in all other circumstances.

SECURITY SAFEGUARDS

Security Safeguards are overseen by the facility's HIPAA officer. These include administrative and physical safeguards that are used to protect the confidentiality and security of PHI in all of its forms (verbal, written, electronic, etc.)

Some of these safeguards may include:

- Workplace security rules regarding access to PHI which may include different levels of access for different workers, vendors, or other contractors.
- Workstations where PHI is used are set up away from public access areas.
- Sign in sheets for visitors and ID badges to identify vendors, visitors, or other non-employee personnel.
- Development of security passwords and policies to maintain the confidentiality of passwords and lockout procedures for terminated employees.
- Detection systems to prevent or correct breaches in security.
- Monitoring technology to access who is accessing PHI, when and how it is used. Also technology to
- validate passwords and pins for electronically shared PHI.
- Authenticating technology, encryption software for electronic transmission, and security software on
- internet web sites and virus checking software to protect the integrity of PHI.
- Policies on how to handle the reporting of security breaches and violations of HIPAA rules.
- Development of backup systems in case of emergencies or disasters that may damage PHI.
- Development of auditing and evaluation procedures to monitor compliance with HIPAA rules.
- Physical locks or limited access areas where PHI is stored.

As the health care professional, your responsibility is to be aware of your specific facility HIPAA rules and security guidelines and adhere to those policies. Logging out of your workstation when done accessing information and protecting the privacy of your password are two basic simple rules to follow at all times.

NOTICE OF PRIVACY PRACTICES

Patients have the right to adequate notice concerning the use/disclosure of their PHI on the first date of service delivery, or as soon as possible after an emergency. And new notices must be issued when your facility's privacy practices change.

PATIENT PRIVACY RIGHTS

The Privacy Rule grants patients new rights over their PHI in all its forms. It's your job to make sure they can exercise their rights, including the following:

- Receive Notice of Privacy Practices at time of first delivery of service.
- Request restricted use and disclosure, although the covered entity is not required to agree.
- Have PHI communicated to them by alternate means and at alternate locations to protect confidentiality.
- Inspect and amend PHI, and obtain copies, with some exceptions.
- Request a history of disclosure for six years prior to the request, except for disclosures made for treatment, payment, healthcare operations or with prior authorization.
- Contact designated persons regarding any privacy concern or breach of privacy within the facility or at HHS.

Parents have the right to access and control the PHI of their minor children – except when state law overrides parental control. Examples include:

- HIV testing of minors without parental consent.
- Cases of abuse.
- When parents have agreed to give up control over their minor child.

PENALTY FOR NON-COMPLIANCE

In addition to potential termination of your employment, if you violate the Privacy Rule, HIPAA set civil and criminal penalties including:

- A $100 civil penalty up to a maximum of $25,000 per year for each standard violated.
- A criminal penalty for knowingly disclosing PHI – a penalty that may escalate to a maximum of $250,000 for conspicuously bad offenses.

PROTECTING PATIENT'S PRIVACY AND THE SECURITY OF THEIR PHI

HIPAA protects our fundamental right to privacy and confidentiality. That means HIPAA's Privacy and Security Rules are everyone's business – from the CEO to the healthcare professional to the maintenance staff. To do your part:

- Make sure you fully understand your facility's privacy practices.
- Protect your computer login and passwords, do not give them out to anyone else to use.
- Protect your patient's personal health information.
- Encourage others to do the same.
- Report any security incidents or violations immediately to your supervisor.

Protecting private patient information is EVERYONE's job in the healthcare setting.

HIPAA Acknowledgement & Confidentiality Agreement

As an employee of **Spherion Staffing & Recruiting** with the potential to take assignments at various health care facilities, I acknowledge that I may receive or have access to confidential patient information in the course of providing services. I understand that it is my responsibility to protect the confidentiality of each client organization's patient records and information including protecting the confidentiality of any electronic or computer passwords that may be assigned to me. I understand that all information pertaining to the diagnosis, treatment and progress of all patients is confidential. I may not review, discuss, copy or transmit such information except where necessary in the normal and proper course of my job. I shall maintain the confidentiality of Private Patient Information (PHI), and in doing so, shall comply with all applicable state and federal laws and regulations, including, without limitation, the privacy provisions under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the policies and procedures of the health care facility to which I am assigned. My agreement to maintain the confidentiality of Private Patient Information shall survive the termination of my employment with **Spherion Staffing & Recruiting** and the conclusion of any assignment(s) at healthcare facilities to which I have been assigned.

I acknowledge my responsibility to report to the facility HIPAA officer and **Spherion Staffing & Recruiting** any potential breach of HIPAA which may include any unauthorized, unintended or inappropriate use or disclosure of confidential patient information either due to my actions or the actions of others.

This policy applies to all patient records and confidential information.

I understand that any violation of this confidentiality policy or breach of HIPAA law shall constitute grounds for disciplinary action up to and including termination of my employment.

I have read and understand the significance of this policy and agree to abide by its provisions.

_____

Employee Name (print) Date

_____

Employee Signature