Health Insurance Portability and Accountability Act

HIPAA Compliance Handbook for Healthcare Staffing Agencies

SUNHEALTHCARE

Caring is the Key in Life

Mission, Core Values and Scope

Sun Healthcare Group

Mission

Caring is the Key in Life.

Our mission statement succinctly defines our purpose as healthcare providers and our commitment to our patients, families and communities. We care about our service, we care about those with whom we serve and ultimately we care about those who receive our care.

Core Values

With this mission, the following four core principles guide our company:

1. Our employees are the company.
   Quality care is our bottom line.
2. Surpass all expectations.
3. Ownership and accountability
4. Serve the customer.

Scope

This handbook applies to employees, volunteers, students, officers and directors of Sun Healthcare Group, Inc. and employees, volunteers, students, officers and directors of any of its directly or indirectly owned subsidiary entities. References in this handbook to "Sun Healthcare Group," "Sun" or "The Company" mean Sun Healthcare Group, Inc. and/or its affiliates, as the context may require. References in the handbook to "employees" means employees, volunteers, students, officers and directors, as the context may require.

Throughout this handbook, we have tried to use language and references that apply to each of Sun's lines of business. The term "patients" refers to the residents and patients who receive the many types of healthcare services that the affiliates of Sun Healthcare Group, Inc. provide.

PART I Introduction

As a part of Code of Conduct training, you learned about the need to respect patients' rights, including the right to confidentiality concerning personal, medical and financial information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that defines patients' rights to privacy and control of how their personal healthcare information is used. This healthcare information is commonly referred to as protected health information (PHI). The law specifies who may access patients' protected, identifiable health information and when disclosure of this information is permitted.

HIPAA's Privacy Rule:

- restricts the way personal health information may be used and disclosed;
- gives patients greater access to their medical records; and
- provides greater protection for patients' medical and financial records.

This law affects healthcare providers, such as nursing homes, hospitals, hospices, pharmacies, laboratories, rehabilitation agencies, healthcare staffing providers and home health agencies, as well as healthcare clearinghouses and health plans. The government refers to these as covered entities (CE). In addition, our business associates must follow this law. A business associate is a person or organization that performs a function on behalf of the covered entity that involves the use of PHI. Business associates include certain physicians, such as medical directors; temporary and contract staff; billing entities; plaintiff or outside attorneys; and others who work with or in Sun companies. As an employee of a Sun affiliate that provides healthcare services, you must know your responsibilities and obligations under this law.

This handbook is part of your training about HIPAA rules. You may have also seen a video or participated in on-line training. Every employee and regular volunteer must participate in HIPAA training during orientation.

PART II How Does HIPAA Affect Patients and Residents?

HIPAA expands patients' rights over their PHI and how it is used. HIPAA gives patients the right to:

- receive a copy of the Notice of Privacy Practices (NPP);
- request changes and amendments to their PHI;
- request PHI be communicated or delivered to them by an alternative means;
- request access to their PHI;
- know where, when and to whom their PHI has been released;
- restrict the disclosure of PHI; and
- report violations to the company and/or the United States Office of Civil Rights.

Patients must receive a clear, written explanation of how healthcare providers may use and disclose their Protected Health Information (PHI). This form, called the Notice of Privacy Practices, is included in the admissions packet or provided to the patient on the first date of service, visit or encounter.

This initial agreement gives examples of how and when information may be disclosed. The patient may object to any of the uses described in this document. The entity may not always be required to abide by the objection, but each objection must be addressed. The patient or his/her legal representative must give additional authorization whenever information is disclosed in any situation that is not defined in the initial agreement.

Unless the information is used for treatment, payment for treatment or center operations, only the patient and individuals specifically authorized by the patient may access or authorize the release of his or her PHI.

Notes

PART III What is Protected Health Information (PHI)?

Protected Health Information is any information that can both identify an individual and link that individual to information regarding his or her medical condition. Information that can identify an individual includes:

- name;
- address;
- social security number;
- employer;
- relatives' names;
- date of birth;
- phone/fax number;
- e-mail address;
- medical record number;
- member/account number;
- certificate and license numbers;
- dates, such as admission, discharge or death;
- vehicle identifiers, including license numbers;
- voiceprints;
- fingerprints;
- photographs;
- codes; and
- anything else that may identify the individual.

Medical information includes:

- past, present or future physical or mental condition;
- past, present or future provision of care; and
- past, present or future payment for care.

Any combination of information from these two lists qualifies as PHI.

PART IV Safeguarding Protected Health Information: Your Responsibilities

Because we work in a healthcare environment, we may have access to private, personal, medical and financial information about the patients in our care. Of course, we need access to this information to do our jobs properly, but we have a legal and ethical obligation to keep patient and employee medical information completely confidential and to limit access to this information to a "need-to-know" basis.

Patient information is exchanged in verbal, written and electronic forms. On the job, we communicate in many different ways and situations: meetings, reports, medical records, face-to-face and telephone conversations, faxes, written reports, documentation, white boards and electronic records. HIPAA regulations require that we take steps to protect any identifiable information from being seen, heard or read by anyone who is not authorized to do so.

The law applies to information that you use to do your job and to any information you may overhear, read or learn accidentally. Because you are an employee in a health-related environment, even casual conversations may not be repeated. Every employee, no matter what his or her job responsibilities, must actively protect PHI.

You must protect all verbal, written, or electronic information that you use as part of your job by taking precautions to ensure that:

- all conversations about patient and employee medical information occur in a secure area where others cannot overhear you;
- all written and electronic information is covered, closed or put away so others cannot see it; and
- all PHI not required to be maintained per regulation or policy is shredded or otherwise destroyed before disposing of the information, including, but not limited to, any document, note or post-it with PHI.

You must avoid seeing, hearing or reading any PHI that you do not need to perform your job responsibilities. If you accidentally obtain information you should not have, like a fax picked up with other papers, tell your supervisor and treat it as confidential.

You must not share information in verbal, written or electronic form with anyone who is not authorized to have it. This includes well-meaning family members, friends, reporters and any others who inquire about a patient or employee who are not specifically authorized by the patient or employee. This also includes your own friends and family members. Unauthorized photography or recordings and disclosure of patient information on Internet-based chat rooms, blogs or social network web sites violate HIPAA regulations and our *Code of Conduct*.

PART V Access to PHI

Three categories of individuals are permitted to access PHI:

- the patient;
- individuals specifically designated by the patient; and
- staff, consultants and others involved in the care and treatment of patients, payment for care and treatment, and healthcare operations. This includes business associates such as billing companies who need access to PHI in order to bill appropriately.

Patients

Patients have the right to be informed fully about their care and treatment. They may access their medical records at any time. Records must be provided to the patient on request.

In addition, patients may request to amend or change information in their medical records. If patients believe their records are inaccurate, they may propose amendments for review.

Patients also have the right to see a list of where and to whom their PHI has been released. The entity must maintain accurate records regarding the release of such information and have them available on request. This is called an accounting of disclosures.

Authorized Individuals

Authorization means that the patient has specifically designated the person as someone who may receive PHI. The patient may authorize family members, friends and other interested parties, such as attorneys, to be informed about the patient's care. Authorization must be documented on the entity's authorization form. While a written authorization is always preferable, you may encounter situations where only a verbal authorization can be obtained. If this is the case, the authorization must be explained and documented on the entity's authorization form.

No information may be provided to anyone who is not specifically authorized by the patient. This includes family members, friends, reporters and anyone else who inquires about the patient.

Staff

Staff may access PHI when they need the information to provide care, arrange for payment and complete entity operations. This access is strictly on a "need-to-know" basis. If you need to see patient or employee information to perform your job – as nurses, rehabilitation therapists and billing clerks do – you are allowed to do so.

Access to PHI is permitted when the information is used for:

- providing treatment/care including, but not limited to, diagnosis, treatments and medications;
- providing payment for treatment; and
- general entity or corporate operations.

Employees do not have the right to see all information about every patient or employee. For example, a physical therapist treating one patient has no right to look at the medical records of other patients unless he or she is caring for them as well.

PART VI Release of Protected Health Information (PHI)

A consent form and Notice of Privacy Practices that specifies who may use and disclose PHI are part of the admission intake documents. Consent is necessary to disclose information needed for treatment, payment and healthcare operations.

You may also receive requests from individuals and organizations to release PHI. Those requests must be directed to the entity management.

PHI may be released without additional authorization when the information is requested:

- by the patient, legal representative or guardian;
- for treatment, payment or healthcare operations; and/or
- as part of required disclosures to the U.S. Department of Health and Human Services.

Authorization is required for anyone else who requests access to the patient's health information. The law also requires that those who have had access to the patient's records be tracked and that this information be provided to the patient upon request.

Certain activities, such as research, marketing and fund-raising, have special requirements. Some state laws are more stringent and provide additional privacy protections for the patient.

If you receive a request to release PHI, please consult your supervisor, the entity administrator or the privacy officer.

Notes

PART VII HIPAA and Your Job

Every employee, whether treating patients, working in an office or serving in some other role within the company must actively protect PHI. The following section discusses specific responsibilities for your work area.

Office-based and Field-based Employees

Staff, in performance of support functions, may have access to patients' protected health information to fulfill their job functions. To comply with HIPAA regulations, corporate staff must:

- only access PHI necessary to do their jobs;
- follow specified procedures for release of PHI;
- exercise caution when transmitting PHI via e-mail by including only the minimum amount of information required and by ensuring that the e-mail is sent only to appropriate recipients with a need to know;
- use and safeguard passwords and screen savers to protect patient and employee information that is stored and transmitted electronically;
- ensure that data back-up and disaster recovery plans are in place;
- ensure that business associate contracts are in place according to HIPAA requirements for any individuals or organizations who have access to PHI for Sun's patients;
- ensure that all conversations about patient and employee information are private and confidential at all times;
- ensure that any stored PHI can only be accessed by the appropriate personnel;
- shred or destroy PHI before disposing information not required to be maintained per regulation or policy, including, but not limited to, any document, note or even post-it note with any PHI; and
- never repeat or refer to any information about patients or employees in casual or social situations.

Notes

PART VIII If You Have Questions

When you have completed your training, you should know:

- how HIPAA affects patients;
- what is included in protected health information (PHI);
- how to protect PHI;
- who has the right to access PHI; and
- what must be done before PHI can be released.

If you have any questions about PHI, your access, patients' rights, appropriate disclosure or any other issue related to HIPAA and your job, please talk with your supervisor or the entity's privacy officer.

Violating HIPAA regulations may include civil and/or criminal penalties, with fines up to $250,000 per incident. If you observe or suspect that a coworker is not following HIPAA regulations, you should follow the Four-Step Reporting Process.

Four-Step Reporting Process

1. First talk to your supervisor.
2. If you are not comfortable talking with your supervisor or are not satisfied with the response you receive, talk to another member of the management team or someone from the human resources department.
3. If you still have a concern, contact the compliance department directly.
4. If none of these steps resolves your questions or concerns, or if you prefer, call the toll-free Sun Quality Line at (800) 761-1226. You may call 24 hours a day, seven days a week. All calls are confidential and you may call anonymously if you choose.

PART IX Case Studies for Discussion

Review the following situations to identify potential problems and how to avoid them.

An agency therapist sees at the grocery store the charge nurse from a recent center assignment. The therapist has been off work for several days and asks about one of the patients who is terminally ill. The colleagues discuss the patient's condition and how long he is expected to live. A store clerk overhears their conversation about the patient, who happens to be a family friend. Upset by what she hears, the clerk tells her friend.

Do you think the center staff intended to do something wrong?

Who has the right to tell neighbors and friends about the patient's condition?

How should this situation be handled to avoid violating HIPAA privacy protections?

Mr. Williams and Mr. O'Hara have been roommates in the center for two years after a life-long friendship. Mr. Williams was taken to the hospital four days ago. Mr. O'Hara's daughter asks the agency COTA about Mr. Williams, saying that she and her father are very concerned about their friend. The COTA happens to know the daughter well and wants to reassure her.

What should the COTA tell Mr. O'Hara's daughter?

What should the COTA not tell Mr. O'Hara's daughter?

What else would you do?

An agency registered nurse accidentally picks up a fax meant for another nurses' station. The fax includes medical information about a new patient who has been admitted with tuberculosis. The agency nurse becomes worried because she knows that her neighbor is in the hospital and will share the same room with the new patient.

What should she do?

How should she avoid this situation?

Have anyone's rights been violated?

An agency therapist is completing data entry into the computer in the rehab department. She hears a patient calling and gets up to assist, then is distracted by a family member on her way back. While she is away from the computer, the center marketing director has been giving a tour to the family of a prospective patient. While they stop to talk in the rehab department, one of the family members has been reading the information on the computer screen and asks about the identity of the patient. He thinks he might know him from church.

What would you say to the visitor?

How do you prevent this situation from happening again?

An agency nurse has been placed on a 13-week charge nurse assignment and wants to put up a bulletin board with photos of current and former patients who have met their goals and been discharged.

Does she need to get permission from the patients to include their pictures?

A patient's neighbor is visiting. On her way out, the visitor stops by the therapy department where the agency therapist is assigned. Very worried, she asks about her friend's condition, her prognosis, the family's discharge plans and the cost of her treatment.

What would you say to the visitor?

The local mayor's mother has been admitted to the hospital's intensive care unit after being in an auto accident. You are an agency nurse assigned to the intensive care unit. Your husband is a reporter for the local paper and calls you at work to ask about the mayor's mother.

What do you do?

Mrs. Bridges has been diagnosed with terminal cancer. Her daughter is visiting from out-of-state. When you enter the room to provide treatment to your next patient, you see the patient is asleep and the daughter is reading information about positioning that was left for the patient earlier in the day. The daughter tells you she is a physical therapist and wants to know what therapy services her mother is receiving and why. It is clear she is distraught and ready to explode.

How would you respond?

Who has the right to know Mrs. Bridges' medical information?

Patty is an OTR who has been working on positioning and ADLs with her patient. Now the patient is beginning to be able to participate but needs setup for the ADLs and assistance with positioning. Patty wants to put up a reminder for the ADLs and a photo of how the patient should be positioned in her room.

What problems could occur?

What should she do instead?

Sue Miller is a staffing manager in a CareerStaff branch office. Sue has a cousin who is a patient at one of the branch client facilities. The daughter of the cousin contacts Sue about how much the medical care is costing and even sends her some of the sample bills. Sue know that her cousin, the patient, is competent, yet Sue feels she should discuss with the family about the cost so they can monitor the patient's expenses more closely.

Is Sue authorized to share/discuss information with the family?

What should Sue do?

Bob Sanchez is a staffing manager at a local branch office. He receives an e-mail from a home health agency client requesting temporary staff for a new home care patient. That patient information includes PHI.

Is it appropriate to e-mail PHI to the healthcare staffing agency?

What should Bob do with this information?

A local mortgage company calls a CareerStaff branch office to confirm employment and length of service for a previous employee.

Under HIPAA, are you allowed to release this information?

Notes

HIPAA Words You Should Know

Term/Abbreviation	Definition
Authorization	A patient's statement of agreement to the disclosure of protected health information (PHI) to himself/herself or to a third party.
Business Associate (BA)	A person or organization who provides a function or activity that involves the use or disclosure of PHI on behalf of one of Sun's companies.
Covered Entity (CE)	A healthcare provider that transmits healthcare information using one of the standard transactions as defined by the U.S. Department of Health and Human Services. An example of this would be billing Medicare or Medicaid electronically for services you provide. If you do this, your agency, center, hospital or operation is a covered entity.
Designated Privacy Officer (DPO)	The manager of your center, entity or area who is charged with the responsibility for overseeing the implementation of the HIPAA training and compliance. This person is your resource for information, questions, concerns and reporting.
Protected Health Information (PHI)	Information that is a subset of health information, including demographic information, and: • is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and • relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; and ▪ identifies the individual; or ▪ has a reasonable basis for believing the information may be used to identify the individual.

Cuts here →

Perf as shown. Do not print perf lines or cut lines.

Folds Here →
Do not print.

Protected Health Information (PHI)

PHI is individually identifiable health information relating to the care and treatment (past, present, future) of the individual, as well as payment for his or her care and treatment.

To be considered "individually identifiable health information," it must identify the individual or there must be a reasonable basis to believe the information can be used to identify the individual. Examples include name, address, date of birth, social security number, diagnosis or admission date.

Patients' Rights

Patients have the right to:

- receive our Notice of Privacy Practices;
- request amendments to their PHI;
- request PHI be communicated in an alternative manner;
- access, review and obtain a copy of their PHI;
- request an accounting of disclosures of their PHI;
- request use and disclosure restrictions of their PHI; and
- file a complaint with the designated privacy officer, Sun's privacy officer or the Office for Civil Rights.

Use and Disclosure of PHI

Patient authorization is not required for:

- treatment;
- payment;
- healthcare operations;
- reasons of national security;
- complying with laws;
- healthcare oversight agencies;
- law enforcement officials;
- funeral directors or coroner;
- FDA, public health department or protective agencies;
- military (for active service or veterans); and/or
- correctional institutions (for convicts).

Patient authorization is required for:

- attorneys;
- researchers;
- marketing; and/or
- fund-raising activities.

– over –

Protected Health Information (PHI)

Your Responsibilities

You have the responsibility to:

- obtain the patient's authorization for any use or disclosure as required;
- use or disclose the minimum amount of PHI necessary to perform your job;
- use reasonable safeguards to protect the privacy of patients and their PHI;
- use precautions when transmitting, sending or receiving PHI;
- abide by the terms of our Notice of Privacy Practices and Sun's privacy policies;
- keep all of your logon IDs and passwords confidential;
- keep your computer free from unauthorized software;
- limit discussions of patients' PHI to authorized individuals or those directly involved in patients' care; and
- report any suspected violations using the Four-Step Process.

Safeguards

As a means of protecting PHI, be sure to:

- perform regular back-ups for all local desktops and servers;
- position computer monitors, printers, fax machines and photocopiers away from public view or access;
- position whiteboards and other posted documentation containing PHI away from public view or access;
- maintain medical/clinical charts behind the nurses' station away from public view or access;
- close MARs and TARs when not in use and store carts in an area away from public view or access;
- protect PHI by always sending it in an envelope or folder, whether within or outside your center, such as for a doctor's appointment;
- shred any paper document with PHI, as well as labels on IVs and medication bottles, before discarding;
- strike through PHI (when it can not be removed and shredded) using an indelible, black marker before discarding; and
- when PHI is not in use, or if record keepers are not present, lock file cabinets or offices where PHI is stored.

SUNHEALTHCARE

Caring is the Key in Life

18831 Von Karman, Suite 400
Irvine, CA 92612

April 2009

090081 7.5K 4/09