



CARE STAFFING

Professionals

CONTRACT EMPLOYEE – REGISTRY STAFF CONFIDENTIALITY PLEDGE

Patient and employee information from any source and in any form (such as paper, talking, computers, etc.) is confidential. I shall protect the privacy and confidentiality of patient and employee information. Access to this information is allowed ONLY if I need to know it to do my job.

In my job, I may see or hear confidential information on:

- **PATIENTS AND/OR FAMILY MEMBERS**

Such as patient records, conversations and financial information

- **EMPLOYEES, VOLUNTEERS, STUDENTS, CONTRACTORS, PARTNERS**

Such as salaries, employment records, disciplinary actions

- **BUSINESS INFORMATION**

Such as financial records, reports, memos, contracts, CHHP computer programs, technology

- **THIRD PARTIES**

Such as vendor contracts, computer programs, technology

- **OPERATIONS IMPROVEMENT, QUALITY ASSURANCE, PEER REVIEW**

Such as reports, presentations, survey results

I AGREE THAT:

1. **I WILL ONLY** access information I need to do my job.
2. **I WILL NOT** show, tell, copy, give, sell, review, change or trash any confidential information unless it is part of my job. If it is part of my job to do any of these tasks, I will follow the correct department procedure (such as shredding confidential papers before throwing them away).
3. **I WILL NOT** misuse or be careless with confidential information.
4. **I WILL KEEP** my computer password secret and I will not share it with anyone.
5. **I WILL NOT** use anyone else's password to access any CHHP system.
6. **I AM RESPONSIBLE** for any access using my password.
7. **I WILL NOT** share any confidential information even if I am no longer working at CHHP.
8. **I KNOW** that my access to confidential information may be audited.
9. **I WILL** tell my supervisor if I think someone knows or is using my password.
10. **I KNOW** that confidential information I learn on the job does not belong to me.
11. **I KNOW** that CHHP may take away my access at any time.
12. **I WILL** protect the privacy of our patients and employees.
13. **I WILL NOT** make unauthorized copies of CHHP's software.
14. **I AM RESPONSIBLE** for my use or misuse of confidential information.
15. **I AM RESPONSIBLE** for my failure to protect my password or other access to confidential information.
16. I have received a copy of and have read the policy Confidentiality of Patient Information and I AGREE TO ABIDE BY IT.

Failure to comply with this agreement may result in the termination of my contract employment at client facility and/or civil or criminal legal penalties. By signing this, I agree that I have read, understand and will comply with this agreement.

Signature: _____

Date: _____

Print Full Name: _____

Unit: _____

**EXAMPLES OF BREACHES OF CONFIDENTIALITY
(What You Should NOT Do)**

These are examples only. They do not include all possible breaches of confidentiality covered by this policy and the agreement.

Accessing information that you do not need to know to do your job:

- Unauthorized reading of patient account information.
- Unauthorized reading of a patient's chart.
- Accessing information on yourself, children, family, friends or co-workers.

Sharing your sign-on code and password:

- Telling a co-worker your password so that he or she can log in to your work.
- Telling an unauthorized person the access codes for employee files or patient accounts.

Sharing, copying or changing information without proper authorization:

- Making unauthorized marks on a patient's chart.
- Making unauthorized changes to an employee file.
- Discussing confidential information in a public area such as a waiting room or elevator.

Using another person's sign-on code and password:

- Using a co-worker's password to log in to the Hospital's computer system.
- Unauthorized use of a log-in code to access employee files or patient accounts.
- Using a co-worker's application for which you do not have rights after he/she is logged in.

Leaving a secured application unattended while signed on:

- Being away from your desk while you are logged into an application.
- Allowing a co-worker to use your secured application for which he/she does not have access after you have logged in.

BREACHES OF PATIENT CONFIDENTIALITY

Level I

Inadvertent Breach (Carelessness): Is a breach that occurs when an individual unintentionally or carelessly accesses, review, or reveals patient information to himself/herself or others without a legitimate need to know the patient information. Is accidental, often due to lack of education or awareness. Examples may include failing to log off a computer terminal; discussing patient information in a public area; leaving a copy of patient information in a public area. Often these breaches do not result in actual patient information being exposed or shared. Discipline should include a verbal warning and mandatory re-education for the first offense up to termination for repeated offenses. **These are considered minor infractions.**

Level II

Intentional Breach (Curiosity or Concern): Is defined as accessing a patient record with no legitimate purpose for doing so. This might mean accessing a friend's or relative's record out of curiosity or releasing information inappropriately. Discipline should include a written warning and mandatory re-education and termination for repeated offenses. These are considered a major infraction. **These are considered a major infraction.**

Level III

Intentional Breach With Malice or Personal Gain: Is defined as a breach when an individual accesses, reviews, discusses patient information with the intent to use it for personal gain or to harm someone. **This is considered a critical infraction.** Discipline should be termination for cause.