

POLICIES AND PROCEDURES

DOWNTOWN STREETS

HIPAA AND CONFIDENTIALITY

12/2/10

Definitions:

HIPAA: Health Insurance Portability and Accountability Act of 1996; HIPAA effective date April 14, 2003

Covered Entities or CE's: A covered entity contracts with a person /entity to help with its own operations and the contracted work requires access to or use of "protected health information". A Business Associate Agreement is required.

PHI: Protected Health Information is defined as "individually identifiable health information" created or used by covered entities.

ROI: Release of Information signed by the patient/client allows release or exchange of PHI

EMR: Electronic Medical Record

Treatment: Means the provision, coordination, or management of healthcare and related services by one or more health care providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between health care providers relating to a patient, or referral of a patient for health care from one health care provider to another.

Covered Entities and Business Agreement Requirements

- Provide Notice of Privacy Practices to patients/clients
- Policies and procedures written and staff trained
- Appoint a Privacy Officer-Program Manager Downtown Streets
- Appoint a Security Officer-Program Manager Downtown Streets
- Secure records that contain PHI so there is no unauthorized access or use-case

files are housed in locking file cabinets inside a locked chart room.

- Account for specific disclosures
- Establish a complaint mechanism-First line of complaint to Case Manager, then Program Manager, then Project Consultant
- Establish and enforce a system of sanctions for employees who violate privacy policies and procedures-See below Privacy Rule/Confidentiality
- Mitigate harm if there is an unauthorized access, use or disclosure
- New HITECH Act rule: Notify patients and government agencies in the event of a breach

Privacy Rule/Confidentiality

Basic Rule: Never use, access, or disclose PHI unless ***there is a law that says you must or a law that says you may***

*Minimum Necessary rule:

When you do use, access or disclose PHI, limit it to the “minimum necessary”. *Does not apply when use, access or disclosure is for ‘treatment purposes.’

Other Confidentiality Laws:

- If another state or federal law also protects confidentiality, then compare the two, and if no conflict between the two, follow: The stricter law when it comes to protecting privacy, and the most “generous” law when looking at the patient rights
- Under HIPAA now, patients always have a right to see their records unless deadly or serious physical harm could result. This includes harm to staff members.

HIPAA says you MUST disclose in 2 circumstances:

1. Request from Secretary of the Department of Health and Human Services
2. Request from client seeking access to his or her own records.

HIPAA says you MAY disclose in some cases:

1. Without the need for permission:

- Child abuse/neglect; elder/dependent adult abuse or neglect. It is noted that all residents of 24 hour care facilities, at the time of residence, are considered dependent adults.
- Gunshot or suspicious injury-Downtown Streets staff will encourage client/patient to see ER, clinic medical staff, physician or physical health provider. The medical staff are the required reporters in this instance. This includes domestic violence.
- Tarasoff “Duty to Warn”:
 - a. Downtown Streets staff will discuss immediately with supervisor any concerns which arise related to threats by a patient/client to another individual.
 - b. Downtown Streets staff will document in the progress notes exactly what has been stated.
 - c. Supervisor will consult with Risk Manager as needed.
 - d. If possible, a letter will be sent to the person who has been threatened and if there is a change in the situation, another letter should be sent to advise the threat has been cleared.
- Infectious reportable conditions: Downtown Streets staff may cooperate with Public Health officials regarding locating individuals where there are infectious disease concerns such as TB.
- Mental health information to law enforcement for the protection of constitutionally elected officials
- Release of 5150'd individual if requested on 5150 hold by law enforcement
- If required by subpoena or Court Order, records including general health information may be released without permission. ***Under California law, a subpoena is***

enough for general health information, but a Court Order is also required to release mental health, drug and alcohol and HIV information. The practice will be to take any record which contains mental health, drug/alcohol or HIV information to court. If the judge orders, the information can be provided.

- For purposes of treatment, payment or operations TPO: a. This is an area where information is shared for coordination of care. Some California and Federal Drug and Alcohol programs restrict sharing of information in a manner that is more restrictive than HIPAA. b. See Definition of “Treatment”. Referrals from hospitals or medical respite are covered under this definition
- When information is de identified i.e. there is no personal information provided. The data provided to grantors would be included in this permission
- When disclosure is incidental, again data is acceptable if not PHI.

2. With opportunity to object, and no objection is voiced

- **Hospital registry**
- **Inquiry form the media (if patient name is given): Hospitals can provide condition if the name is given by the caller**

3. With permission from the client (“written authorization”)

- **All other third party disclosures are permitted if permission from the patient. Downtown Streets staff will obtain specific written releases for these disclosures using the appropriate Release of Information forms.**
- **Normally disclosures to a third party will not occur unless there is written authorization on a HIPAA compliant form.**
- **Often hospitals and other CE’s will insist on using their own forms for PHI. It is the policy of Downtown Streets to obtain relevant HIPAA forms to keep on file as needed for CE’s to release information.**

Getting Permission-must it be in writing?

- Verbal permission is ok under some circumstances, e.g. when you are in the same room with the client and the third party
- If someone calls and makes a request for their own information, using reasonable caution to verify identity
- If unsure who is calling and requesting third party disclosure, send a form and have it signed and returned.

If CE refuses to send records or discuss information:

- **Have client “access” their own record**
- **Remember this is a MUST disclose under HIPAA**

Duty to Mitigate Harm

- Privacy rule required CE’s i.e. health care providers to mitigate to the extent practicable, any know harmful effect of improper disclosure
- The rule did not specify what is involved, so each situation needs to be assessed individually

Duty to Apply Sanctions

- Sanctions applied under the Downtown Streets program will be proportionate to the infraction
- If there is a deliberate breach such as looking up an ex-husband’s girlfriend or VIP’s PHI with the access available, this will likely be cause for termination especially if this information is used in some way that is harmful.
- If someone looks at a record of a patient she used to work with, but no longer does, because the need to know rule is misunderstood, a short suspension may be appropriate
- If someone picks up the wrong chart and reads it accidentally, then no sanction will be imposed except a verbal warning.

Risk Assessment and Analysis

- **Downtown Streets receives and maintains PHI from health care providers. This information is used to provide intensive case management services to our clients.**
- **All PHI that is received is put into individual client files which are maintained in a secured records room in locked file cabinets. The records room is locked after business hours at all times and its entrance is supervised during business hours at all times. The specific keys for the file cabinets are maintained at a central desk and are always subject to the control of the Administrator or designee.**
- **Files are only to be accessed by staff with a “need to know” based upon their job function.**
- **Any PHI which is obtained electronically is password protected. The Santa Clara County computers utilized by all Downtown Streets staff are password protected. The individual programs available from the CE hospitals are also and additionally password protected.**
- **All laptops and computers are protected according to NIST standards, so even if lost or stolen would not involve a breach of PHI.**
- **On occasion, PHI is created by Downtown Streets staff who provide clinical services and that PHI is similarly protected.**
- **All staff are trained on an annual basis on confidentiality laws and our own policies concerning use and disclosure of PHI that we maintain.**
- **All new staff receive training during the Health and Hospital orientation as well as the Downtown Streets new employee orientation.**
- **All staff sign a confidentiality agreement acknowledging this training and agreeing to abide by Downtown Streets policies and procedures and the law.**
- **Appropriate sanctions are written and applied in case of any breach subject to the review and involvement of the Human Resources Department of the California Hospital Association.**
- **Desk top computers: All Downtown Streets desk top computers are issued and protected by the County of Santa Clara. The screen becomes blank after a few**

seconds to preserve privacy of information on the screen. All computers are password protected.

The HITECH Act

- The HITECH Act has incentive to adopt Electronic Health Records**
- There will be penalties in the future for failure to adopt HER systems, and**
- Stricter privacy and security provisions**

Breaches are emphasized in the HITECH Act

Patient rights under HIPAA and HITECH Act

- 1. Right to access the chart/EHR**
- 2. Right to Accounting of Disclosures-these are maintained for three years for electronic records**
- 3. Right to Correct Errors-patients must be allowed to review their own records upon request and to request correction of errors in their records.**
- 4. Right to Restrict Disclosures-if care is paid for with cash, no disclosure to the insurance companies can be made.**