



FOR IMMEDIATE RELEASE

North Suburban Human Rights Authority
Report of Findings
Linden Oaks at Edward
HRA #18-100-9019

The North Suburban Regional Human Rights Authority (HRA) of the Illinois Guardianship and Advocacy Commission has completed its investigation of alleged rights violations at Linden Oaks at Edward. The HRA notified Linden Oaks at Edward of its intent to conduct an investigation pursuant to the Guardianship and Advocacy Act (20 ILCS 3955). The complaint accepted for investigation alleged that the protected health information of some outpatient program patients was not secured as the information had been lost in transit.

The rights of mental health patients receiving services at Linden Oaks at Edward are protected by the Illinois Mental Health and Developmental Disabilities Confidentiality Act (705 ILCS 110) and the Health Insurance Portability Act (HIPAA) (45 CFR Part 160 and Part 164).

To pursue this investigation, the HRA requested and reviewed the hospital's policy that pertains to the wrongful disclosure of protected health information. Also requested was education provided to staff members about the proper disclosure and security of patient information. A site visit was conducted, at which time the allegation was discussed with hospital personnel. The HRA acknowledges the full cooperation of hospital personnel.

Background

Edward-Elmhurst Health was created in 2013, when Edward Hospital & Health Services and Elmhurst Memorial Healthcare merged to become one of the larger integrated health systems in Illinois. Linden Oaks Behavioral Health, a part of Edward-Elmhurst Health treats conditions such as anxiety, depression, eating disorders and self-injury for adolescents and adults. According to the web-site, they are a leading center for the treatment of substance abuse and offer services for each stage of the recovery process, including inpatient and outpatient treatment, residential (for adults) and detoxification. Their comprehensive eating disorders program is nationally known and locally preferred.

Findings

As stated above, it was reported that some outpatient program patients' clinical records were not secured, as the materials had been lost while they were being sent from an outpatient site to Linden's Oaks Medical Records Department.

At the site visit, it was explained that treatment data for both inpatient and outpatient recipients are collected electronically. However, some documents like the daily check-in sheets, release of information forms, treatment plans and after-visit summaries are hard-copy documents. When a patient is receiving off-site outpatient services and he/she is discharged and/or the service

status changes, these forms are placed in a locked bag and transported to the Medical Records Department via a courier service.

Hospital personnel stated that upon receiving notification of a patient's service status change, it was discovered by Medical Records that the hard-copy documents for this patient had not been sent to medical records. An investigation was immediately conducted and it revealed that documentation for nine patients were unaccounted. The courier service was contacted as were the other drop-off sites on the route; staff members were interviewed, but despite a thorough investigation, the locked bag could not be located. Hospital personnel also stated that they are not even certain that the documents got into the bag – the error could have occurred prior to that step.

As a result of this incident, corrective measures have been taken to identify process improvements. The courier and staff member now must sign off that he/she has received the documents and have placed them in the locked bag. The courier previously made two additional stops before the documents were delivered. As a corrective measure, the route is now direct; the courier makes no additional stops. The hospital is also in the process of piloting a plan to determine if the documentation can be scanned into the clinical record– this is being conducted at another site. The patients identified were personally contacted by the hospital's President and CEO and advised of the situation. Although they did not believe that the unaccounted documents contained any financial information, the hospital provided one year of free credit monitoring.

In response to the HRA request regarding education provided to staff members about the proper disclosure and security of patient information, materials were given that shows that all employees must complete an annual mandatory privacy and information security training. In addition, new employee orientation is provided which includes training related to patient confidentiality, applicable regulations and the use and disclosure of protected health information. Also provided were the actual training modules.

The hospital's Privacy Breach Notification policy states that a breach is "the unauthorized acquisition, access, use or disclosure of PHI/PII [Protected Health Information/Personally Identifiable Information]: The unauthorized acquisition, access, use, or disclosure of PHI/PII is presumed to be a breach unless the System or Systems' Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on the Systems' risk assessment. Examples of potential breaches include but are not limited to: disclosures of PHI/PII to unauthorized individuals via mail, fax, email, or handling paper PHI/PII to an unauthorized recipient, access, use, or disclosure of PHI/PII for a purpose not consistent with the corporate standard or for a purpose other than treatment, payment, or operations as consistent with HIPAA." The policy includes the measures staff members are to take upon discovery of a potential breach of PHI/PII. To summarize, staff are to report a potential breach immediately following the appropriate chain of command; the Privacy Officer directs an investigation; if a breach did occur, appropriate internal personnel are notified and written notification to any patient affected; if an investigation confirms that a violation has occurred, corrective action may occur, including discipline up to and including termination of employment, contract or relationship; if an employee is found to have inappropriately used, accessed, or disclosed PHI/PII, they may be subject to additional training and discipline up to and including termination.

Conclusion

Pursuant to the Illinois Mental Health and Development Disabilities Confidentiality Act (740 ILCS 110/3) "All records and communications shall be confidential and shall not be disclosed except as provided in this Act. Unless otherwise expressly provided for in this Act, records and communications made or created in the course of providing mental health or developmental

disabilities services shall be protected from disclosure regardless of whether the records and communications are made or created in the course of a therapeutic relationship”.

The HIPAA Privacy Rule (45 CFR Part 160 and Part 164) “establishes national standards to protect individuals medical records and other personal health information. The Privacy Rule applies to health plans, health care clearinghouses, and health care providers that conduct health care transactions electronically. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.”

Based on the information obtained, it is concluded that the protected health information of some outpatient program patients was not secured; the allegation is substantiated. Because this incident was immediately addressed and corrective measures are in place and other measures are being assessed, no recommendations will be made at this time.