HIPAA Update

Presented by:

www.TheHealthLawFirm.com

THE HEALTH LAW FIRM®

Main Office:
1101 Douglas Avenue
Altamonte Springs, FL 32714

Phone: (407) 331-6620
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com

THE HEALTH LAW FIRM®

Today's Lecturers:

Michael L. Smith, R.R.T., J.D.

Lance O. Leider, J.D.

Objective

- Update the various components of Orange County Government on HIPAA Privacy.

Changes to HIPAA

Legislative Changes

1. Health Information Technology for Economic and Clinical Health Act

2. Genetic Information Nondiscrimination Act

Regulatory Changes (HHS & OCR)

1. Omnibus Rule 2013, 78 Fed. Reg. 5566, 5701 (Jan. 25, 2013).
   a) Modify and redistribute Notice of Privacy Practices (NPP) to include:
      i. statement that certain uses and disclosures require specific authorization (psychotherapy notes)
      ii. statement that any use and disclosure not addressed in the NPP requires a written authorization

Regulatory Changes (HHS & OCR)

iii. acknowledgement that individual may revoke and authorization

iv. if the covered entity intends to engage in marketing or fund raising, statement that the individual may opt out of receiving such communications

Regulatory Changes (HHS & OCR)

v. statement that the individual has the right to request restrictions on certain uses and disclosures (covered entity is not required to agree to restrictions)

vi. statement that the covered entity is required to maintain the privacy of PHI and is required to (or will) provide notice of a breach of the individuals unsecured PHI to the individual

Regulatory Changes (HHS & OCR)

b) Privacy and Security requirements extended to Business Associates

c) Sale of PHI without consent prohibited

Regulatory Changes (HHS & OCR)

d) Patient right to receive electronic copy of PHI

   i. reasonable security measures that need to be implemented before transmitting data to patients through unsecured means

e) Limitations on use of PHI for marketing

Special Guidance on HIPAA Privacy in Emergency Situations

PHI may be shared without consent under the following conditions:

a. Treatment
b. Public Health Activities
c. Imminent Danger

Compliance

- OCR will start auditing Covered Entities for Compliance and will be imposing fines for noncompliance.
- Previously, OCR only acted upon complaints. (Auditing should have started but it was postponed)

Security of Healthcare Data

- Ponemon Institute study on Security of Healthcare Data
- Responses from covered entities and BA’s on breach causes, costs and sources of breaches

Specific Cases

- **<u>Stanford Hospital & Clinics</u>-** Impermissible Disclosure: Business Associate (billing contractor) shared PHI of 20,000 emergency room patients with a job candidate as part of a skills test. The job candidate posted the information on a tutoring website seeking help to secure the position. The PHI of 20,000 patients remained posted on the tutoring website for over one year before it was discovered by a patient. Patients filed a class action lawsuit, which was settled for approximately $4.1 million.

Specific Cases

- Springer v. Stanford Hospital and Clinics, Ca. Superior Court, No. BC470577 (2014)

- **Settlement Breakdown:** $3.3 million paid by the business associate ($1.3 million of the $3.3 million for attorneys' fees); $500,000 paid by Stanford to fund educational program on new requirements for business associates; $250,000 – paid by Stanford to cover the administrative costs of the settlement

Specific Cases

- **<u>Employee Accessing Medical Records of Other Employee for Personal Reasons</u>-** A hospital employee's supervisor accessed, examined and disclosed an employee's medical record. OCR's investigation confirmed that the use and disclosure of protected health information by the supervisor was not authorized by the employee and was not otherwise permitted by the Privacy Rule. An employee's medical record is protected by the Privacy Rule, even though employment records held by a covered entity in its role as employer are not.

Specific Cases

- **Employee Accessing Medical Records of Other Employee for Personal Reasons-** Among other corrective actions to resolve the specific issue in the case, a letter of reprimand was placed in the supervisor's personnel file and the supervisor received additional training about the Privacy Rule. Further, the covered entity counseled the supervisor about appropriate use of the medical information of a subordinate.

Specific Cases

- **<u>Anchorage Community Mental Health Services</u>-** Unpatched and Unsupported software

  Data breach involving electronic PHI. PHI accessed using malware; breach was direct result of ACMHS not following its own policies and not updating its IT resources.

- $150,000 settlement and Corrective Action Plan

Specific Cases

- **Cancer Care Group, P.C.** - Inadequate Risk Assessment:

Data breach involving unsecured electronic PHI. Lost laptop (insert device of choice: thumb drive, smart phone, tablet, watch) and backup tape with unencrypted data.

- $750,000 fine

Also shows the OCR will take into account the general compliance picture of the entity in determining what the fine is.

Specific Cases

- **<u>Impermissible Uses and Disclosures to Employer</u>** –

  Covered Entity disclosed protected health information to a patient's employer without authorization. Among other corrective actions to resolve the specific issues in the case, including mitigation of harm to the patient, OCR required the Center to revise its procedures regarding patient authorization prior to release of protected health information to an employer. All staff was trained on the revised procedures.

Specific Cases

- **<u>Impermissible Uses and Disclosures in Response to Subpoena</u>** –

  Covered Entity impermissibly disclosed the protected health information (PHI) of one of its patients in response to a subpoena (not accompanied by a court order).

Specific Cases

- **<u>Impermissible Uses and Disclosures in Response to Subpoena</u>** – Covered Entity failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order as required by HIPAA Privacy Rule. Not all subpoenas are equal so Covered Entity must ensure that subpoena meets Federal and Florida requirements before disclosing PHI.

Questions?

THE HEALTH LAW FIRM®

Main Office:
1101 Douglas Avenue
Altamonte Springs, FL 32714

Phone: (407) 331-6620
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com