3.04 HIPAA Compliant Employee Sanctions: A Fair and Objective Approach

Presenter:

Frank Ruelas, MBA

Director, Corporate Compliance
Gila River Health Care Corporation
Sacaton, Arizona

Some views on enforcement…

"It's about time law enforcement got as organized as organized crime.

- Rudolph W Giuliani

Add Visibility to Enforcement Activities

- Maintains awareness
- Increases participation
- Aids decision making
- Deterrent effect

E-E-E-Essential Elements of the Sanctions Policy

Education

Enforcement

Expedient

Equitable

Applies to Privacy and Security

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.

45 CFR 164.530(e)(1)

(C) *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

45 CFR 164.308(a)(1)(ii)(C)

- Coordination aspects
  - Privacy Officer
  - Security Officer
  - Compliance Officer

Key Point # 1:
Define Violation Levels or Categories

Though named differently...

- Level I
- Level II
- Level III

- Type I
- Type II
- Type III

- Group I
- Group II
- Group III

...they share common themes

Level I / Type I / Group I

Cause or Motivation

- Lack of training
- Inexperience
- Accidental
- Unintentional
- No harm no foul

Sanction Activity

- Training
- Counseling
- 3 Strikes Model

Level II / Type II / Group II

Cause or Motivation

- Curiosity
- Concern
- Compassion
- Carelessness

Sanction Activity

- Documentation
  - Warning
  - Counseling
- Notice
- Admin leave
- Probationary Period
- Corrective Action Plan (CAP)

Level III / Type III / Group III

Cause or Motivation

- Malicious Intent
- Financial Gain

Sanction Activity

- Termination

Key Point # 2: Identify Examples for Each Violation Level or Category

Level I / Type I / Group I

Possible themes

- Clerical error
- Technical error
- Judgment error

Examples

- Originals left on copier or fax
- Unopened mail left unattended
- Email address error
- PHI sent to similar named patient
- PHI in conversation overheard
- Desk or work area left unsecured
- Computer files erased
- Computer temporary files not deleted
- Document not placed in shred bin
- Phone messages overheard
- Computer screen left unattended

Level II / Type II / Group II

Possible themes

- Unauthorized
- Not job related
- Stealth mode

Examples

- Checking on patient condition
- Copying information as a favor
- Accessing patient test results
- Installing software
- Experimenting with computer
- Using someone else's password
- Providing access to someone else
- Deleting information from network
- Not following policy or procedure

Level III / Type III / Group III

Possible themes

- Disgruntled
- Theft
- Maliciousness

Examples

- Selling patient addresses
- e-Broadcasting patient info
- Intentionally altering PHI

Key Point # 3:
Link the Violation to the Sanction Activity and Provide Disciplinary Recommendation

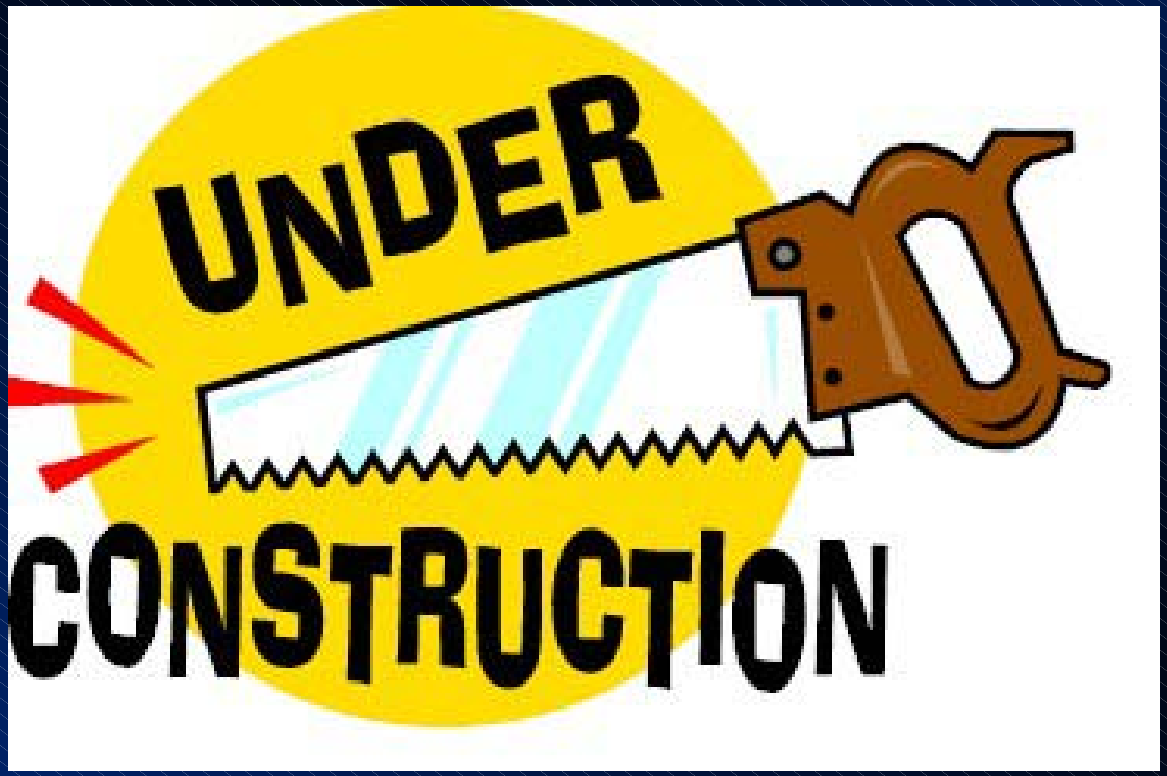
- Provides a high level of objectivity
- Aids in achieving long term consistency
- “Surprise” factor is reduced (eliminated)

Key Point # 4:
Request and Document Activities Performed by Other Departments

- Identifies sanction “creep”
- Validates level of follow through
- Completes file

Key Point # 5:

Under development at print deadline, more to follow…



Summary:

- Enforcement is a critical activity
- Sanctions should be applied consistently
- Remember that mistakes will happen and people learn from mistakes that they make

Email: fruelas@grhc.org