



# HIPAA -- Compliance and Enforcement Issues

---

John T. Bentivoglio  
Arnold & Porter

[john\\_bentivoglio@aporter.com](mailto:john_bentivoglio@aporter.com)

202.942.5508



# Overview

---

- \* HHS approach toward compliance
- \* Compliance procedures
- \* Civil penalties and enforcement
- \* Criminal penalties and enforcement
- \* Private remedies
- \* Internal sanctions



# HHS Compliance Efforts

---

Generally, HHS has pledged a “cooperative” approach to obtaining compliance

- HHS will provide technical assistance
- HHS will seek informal means to resolve disputes

# HHS Compliance Efforts

## Rights of individuals

- Right to file complaints with HHS
- Procedures for complaints modeled on existing procedures for civil rights complaints
- Complainants are protected under so-called “whistleblower” procedures



# HHS Compliance Efforts

---

## Responsibilities of covered entities

- Maintain records
- Provide HHS with access to records (business partners also required to provide access)
- Refrain from retaliation against complainants



# HIPAA Penalties

---

- \* Civil penalties
- \* Criminal penalties
- \* State remedies
- \* Internal disciplinary requirements



# Civil Penalties

“Except as provided in subsection (C),

“the Secretary shall impose on any person who violates a provision of this part a penalty of not more than \$100 for each violation,

“except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000.”.

# Civil Penalties -- Affirmative Defenses

A civil penalty may not be imposed where--

- \* the person did not know, and by exercising reasonable diligence would not have known, of the violation
- \* the failure to comply was due to reasonable cause and not to willful neglect
- \* the failure to comply is corrected within 30 days of discovering the violation

HHS may waive or reduce the amount of a civil penalty and/or extend the 30-day deadline for correction of a violation



# Criminal Penalties

“Wrongful disclosure of IIHI

“Sec. 1177(a). Offense.--A person who knowingly and in violation of this part--

- “(1) uses of causes to be used a unique health identifier;
- “(2) obtains IIHI relating to an individual; or
- “(3) discloses IIHI to another person,

shall be punished as provided in subsection (b).”.

# Criminal Penalties (cont'd)

## Elements of the offense

- Knowledge;
- Violation of Part C (Administrative Simplification); and
- One of the following:
  - uses a unique health identifier
  - obtains IHI relating to an individual
  - discloses IHI to another person

# Criminal Penalties (cont'd)

## “Knowledge” requirement

- The text requires “knowledge” -- not “intent” or “willfulness”
- Arguably, the government is only required to show knowledge of the act -- **not** knowledge that the act was wrongful or unlawful



# Criminal Penalties (cont'd)

---

Unresolved issue -- are business partners (or others) liable under the criminal penalties or are criminal penalties limited to “covered entities”?



# Investigations and Prosecution

---

## \* Investigations

- HHS Office for Civil Rights
- FBI
- HHS OIG

## \* Prosecution

- DOJ

# Criminal Prosecution

DOJ has “independent litigating authority”

- While DOJ will consult with “client” agencies, ultimately Federal prosecutors (AUSAs) decide whether to continue investigate and/or seek an indictment

# State Enforcement Actions

- \* State Attorneys General are not explicitly authorized to bring actions
- \* However, new HHS regulations may bolster existing or create new theories under state laws (e.g., state unfair or deceptive trade practice laws)

# Private Remedies

- \* No private right of action under HIPAA in Federal court
- \* HHS has established procedures for the filing of complaints
- \* Business partner contracts must make data subjects third-party beneficiaries -- which may provide remedies under State law



# Internal Sanctions

- \* Covered entities must develop and apply sanctions for failure to abide by company policies and/or the HIPAA regulations
- \* Range: “warning to termination”.
- \* Sanctions should apply to covered entity’s employees and business partners

# Conclusion

- \* Civil sanctions are modest -- and HHS vows a cooperative approach
- \* Criminal penalties are stiff -- and discretion lies with DOJ
- \* Suits under State law-- either by Attorneys General or private parties -- could be significant (even without HIPAA private right of action)

# Conclusion (cont'd)

---

- \* As with fraud and abuse compliance, comprehensive programs (with support at all levels within the organization) can reduce exposure and risk



# HIPAA -- Compliance and Enforcement Issues

---

John T. Bentivoglio  
Arnold & Porter

202.942.5508

[john\\_bentivoglio@aporter.com](mailto:john_bentivoglio@aporter.com)

October 2000

HIPAA Privacy Summit -- Washington DC