

The Consequences of HIPAA Violations Beyond "Just" Penalties

An IDC infographic sponsored by Sage

HIPAA Violations Can Damage Reputation (In Addition to the Fines)

Patients are the key stakeholders for reputational risk



*Source: Deloitte

Reputation problems have the biggest impact on revenue and brand value

Survey respondents who previously experienced a negative reputation event say the 3 biggest impact areas were:

41%
Revenue

41%
Loss of brand value

37%
Regulatory investigations*

Full Cost of a Violation

HHS reported that the Office of Civil Rights (OCR) had referred 750 cases to the DOJ for criminal investigation as of June 30, 2019*



OCR will refer matters to DOJ for criminal enforcement in some cases or will work cooperatively with DOJ where a DOJ investigation on other grounds reveals a potential HIPAA violation.

A person may be subject to criminal penalties if he or she knowingly (and in violation of HIPAA):



- Uses or causes to be used a unique health identifier;
- Obtains individually identifiable health information relating to an individual; or
- Discloses individually identifiable health information to another person.**

Sources:
* Enforcement Highlights on HHS website hhs.gov
** 2005 Memorandum Opinion for the General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General ("DOJ Memo")

Criminal penalties can include a fine of up to \$250,000 and imprisonment of up to 10 years



Criminal violations range from misdemeanors to felonies

- The highest penalties are incurred if one of these offenses is committed "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm."
- The DOJ Memo explains that "knowingly" refers to knowledge of the facts that constitute the offense, not knowledge of the law being violated (HIPAA).

Source: DOJ Memo

HIPAA Is Serious and Violations Are Corrected

HHS: 98% of complaints are resolved

70% of investigations involved a corrective action

Status of All Privacy Rule Complaints: June 2019		
Complaints Remaining Open	3,969	2%
Complaints Resolved	207,140	98%
Total Complaints Received	211,109	

Total Investigated Resolutions: June 2019		
Corrective Action Obtained (Change Achieved)	27,015	70%
No Violation	11,828	30%
Total Complaints Investigated	38,843	

The Value of Securing Payment Activities

Non-Compliance Carries Significant Risk and Costs

As of June 2019, HHS's Office of Civil Rights has imposed **\$102,681,582** in HIPAA penalties.* (COSTS)



Impermissible Uses and Disclosures is the #1 Type of HIPAA Violation. (RISK)

"Payment" violations fall under Impermissible Uses and Disclosures

Sources: * Enforcement Highlights on HHS website hhs.gov

Patient privacy and data security rules have important implications



Healthcare organizations need to consider the use of PHI carefully in the context of the services their organization provides:

- Having patient contact information alone could be a violation (i.e. Mental Health Services organization)
- Issuing a refund to a patient
- Providing additional services to patients (i.e. clothing or housing allowances)

What You Should Do Now



Expert Advice:

"Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program."

—Leon Rodriguez, Former Director of OCR

Next Steps:

- Review HIPAA privacy and security policies and procedures
- Review business associate agreements
- Issue privacy notices
- Document risk analysis
- Issue training materials
- Review security policies and procedures
- Conduct security risk analysis

