HIPAA Enforcement and Penalties

Go to: How Are HIPAA's Administrative Simplification Rules Enforced? | HIPAA Violation Investigations | Civil Monetary Penalties for HIPAA Administrative Simplification Rule Violations | OCR Enforcement Activities | Criminal Penalties for Intentional HIPAA Violations | State Attorneys General Enforcement | HIPAA Compliance Audits and Best Practices for Avoiding Penalties

Created on: ***12/26/2018***

This practice note discusses the enforcement of the privacy rule, security rule, breach notification rule, and transaction rule under the Health Insurance Portability and Accountability Act (HIPAA) (*Pub. L. No. 104-191*). These requirements are known collectively as the HIPAA administrative simplification rules. Many employers that sponsor group health plans and are involved in plan administration may be subject to all or most of these rules and penalties for noncompliance can be severe. This practice note also provides a summary of enforcement activity in recent years and best practices for covered entities and business associates that handle protected health information to avoid HIPAA violations.

This practice note is organized in the following topics:

For detailed information on the HIPAA administrative simplification requirements, see *HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules*. For additional resources, see the *HIPAA Resource Kit*.

How Are HIPAA's Administrative Simplification Rules Enforced?

Group health plans (including many employer-sponsored group health plans), healthcare providers, and healthcare clearinghouses are all HIPAA covered entities, which must comply with HIPAA's administrative simplification rules. Many of these rules also apply to HIPAA business associates, which are generally service providers that create, handle, or transmit protected health information (PHI) on behalf of HIPAA covered entities. The administrative simplification rules consist of both of the following:

- **Privacy rule, security rule, and breach notification rule (PHI administrative simplification rules).** Each of these rules concern aspects of ensuring the privacy, security, and proper use and disclosure of PHI.
- **Transaction rule.** This rule deals with establishing uniform standards for the electronic administrative transactions, including code set and identifier standards.

The Department of Health and Human Services (HHS) has ultimate responsibility for enforcing these rules. HHS issued enforcement regulations beginning in 2003. See 45 C.F.R. pt. 160, subparts C, D, and E, established by HHS, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings, *68 Fed. Reg. 18,895* (Apr. 17, 2003) (interim final rule) and HHS, HIPAA Administrative Simplification: Enforcement, *71 Fed. Reg. 8,390* (Feb. 16, 2006) (final rule). That rulemaking established the procedural requirements for imposing civil money penalties (CMPs) for violations and clarified:

- The investigation process
- Standards for assessing liability
- Determining penalty amounts
- Grounds for penalty waivers
- Conducting hearings –and–
- Appealing agency determinations

The preambles to the interim final and final rules above provide information that may be helpful regarding HIPAA compliance and enforcement. See *68 Fed. Reg. 18,895–901*, *71 Fed. Reg. 8,390–423*.

The HITECH Act of 2010 (*Pub. L. No. 111-5*) strengthened HIPAA privacy and security rules, enhanced enforcement authority, and increased potential penalties for noncompliance. See *42 U.S.C. § 1320d-5(a)(1)*; HITECH Act § 13410. Among other things, it imposes potential CMP liability directly on business associates for violations of the Act and certain privacy rule and security rule provisions. HITECH Act §§ 13401, 13404. Ensuing interim final regulations and final regulations set the course for HITECH Act implementation. *74 Fed. Reg. 56,123 (Oct. 30, 2009)*; *78 Fed. Reg. 5,566 (Jan. 25, 2013)*.

Responsible Enforcement Bodies

HHS delegated PHI administrative simplification rule enforcement responsibilities to its Office for Civil Rights (OCR) and transaction rule enforcement responsibility to the Centers for Medicare and Medicaid Services (CMS). The regulations and penalties noted above and described in the following sections apply to all administrative simplification rules, but the focus of the remainder of this practice note is on PHI administrative simplification enforcement by OCR. CMS's oversight of transaction rule compliance is generally conducted on an informal basis. For more information on transaction rule requirements and enforcement, see the *CMS Website* and *HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules — What Does the HIPAA Transactions Rule Require?*.

HIPAA Violation Investigations

Enforcement action by OCR can arise from complaints made to HHS or from a compliance review initiated by OCR.

Complaint Requirements

HIPAA grants individuals and entities a right to file complaints regarding compliance with the administrative simplification rules. *45 C.F.R. § 160.306*. Complaints must:

- Be filed in writing, either on paper or electronically, within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless OCR waives this time limit for good cause Name the *person* or entity that is the subject of the complaint –and
- Describe the acts or omissions believed to violate the applicable administrative simplification rule(s)

45 C.F.R. § 160.306(b).

The *HHS website* contains helpful information on the complaint process.

OCR Investigation

OCR is tasked with investigating any complaint that meets the foregoing requirements and is filed against a covered entity or business associate. Investigation is mandatory if the complaint indicates a possible violation due to willful neglect. An OCR investigation may include a review of the pertinent policies, procedures, or practices of the group health plan (or other covered entity or business associate) and of the circumstances regarding any alleged violation. *45 C.F.R. § 160.306(c)*.

Covered entities and business associates must cooperate with OCR complaint and compliance investigations. This includes making available their facilities, books, records, accounts, and other sources of information that are pertinent to the investigations. *45 C.F.R. § 160.310*. See also *HHS, What OCR Considers for Intake and Review of a Complaint*. OCR may issue subpoenas to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review. *45 C.F.R. § 160.314*. OCR also may refer the complaint to the U.S. Department of Justice if the investigation reveals a violation of HIPAA's criminal provisions under 42 C.F.R. § 1320d-6 (e.g., a knowing disclosure of individually identifiable health information). *HHS, How OCR Enforces the HIPAA Privacy and Security Rules*.

Informal Resolution

Upon determining that a HIPAA violation has occurred, OCR may attempt to resolve the case by informal means. This emphasizes HHS's wish to promote voluntary compliance with violations of the HIPAA rules. Informal means may include a showing of demonstrated compliance by the covered entity or business associate or its agreeing on a completed corrective action plan or other agreement. Resolution in this manner can preclude the process by which any potential penalty may be assessed. *45 C.F.R. §§ 160.304*, *160.312(a)*; see *71 Fed. Reg. 8,394–97*.

Most privacy and security rule violations are resolved through an arrangement of this sort between OCR and the covered entity or business associate providing for voluntary compliance, corrective action, and/or entering into a resolution agreement. Where this is the case (or if OCR determines there was no violation), OCR notifies the person who filed the complaint (if any) and the covered entity or business associate to close the case. *45 C.F.R. 160.312(a)(1)*, *(2)*.

Formal Resolution

Where the OCR finds a violation and the matter is not resolved by informal means, it will inform the covered entity or business associate and provide it an opportunity to submit, within 30 days of receipt of the notification, written evidence of any mitigating factors (see “Factors Affecting the Penalty Amount” under *Civil Monetary Penalties for HIPAA Administrative Simplification Rule Violations*) or affirmative defenses (see “Affirmative Defenses” below). If, after reviewing any response, OCR finds that a CMP is warranted, it will issue a formal notice of proposed determination (NOPD). *45 C.F.R. § 160.312(a)(3)*.

Notice of Proposed Determination

OCR assesses a penalty against the covered entity or business associate through the NOPD, which must include:

- A reference to the statutory basis for the penalty
- A description of the findings of fact about the violations (and a statistical sampling if OCR is relying upon a statistical sampling study in accordance with *45 C.F.R. § 160.536*)
- The reason(s) why the NOPD recipient is subject to the penalty
- The amount of the proposed penalty and a reference to the applicable category of the tiered scheme in *45 C.F.R. § 160*. 404 (as described in “CMP Limitations” under *Civil Monetary Penalties for HIPAA Administrative Simplification Rule Violations*)

- Any circumstances considered in determining the amount of the proposed penalty (see "Factors Affecting the Penalty Amount" under *Civil Monetary Penalties for HIPAA Administrative Simplification Rule Violations*) –and–
- Instructions for responding to the notice and information on how to request a hearing to challenge the penalty, discussed in the next section

45 C.F.R. § 160.420(a).

Administrative Appeals

On receiving the notice, the covered entity or business associate can request a review hearing before an administrative law judge (ALJ) but must do so within 90 days of receiving the notice to preserve that right. If the 90-day period elapses without a request, OCR will notify the entity that the fee is final and demand payment. *45 C.F.R. §§ 160.420(b)*, *160.504*.

Affirmative Defenses

OCR may not impose a penalty on a covered entity or business associate if the respondent can demonstrate that the violation:

- Was not due to willful neglect –and–
- Was corrected in a timely manner, meaning:
    - Within 30 days of the first date it knew (or, by exercising reasonable diligence, would have known) the violation occurred –or–
    - During an extended remediation period OCR determined to be appropriate for the violation

45 C.F.R. § 160.410(c).

It is also an affirmative defense to a CMP if the same violation was the basis for a penalty under the HIPAA criminal liability provisions in *42 U.S.C. 1320d-6*. *45 C.F.R. § 160.410(a)(2)*.

Settlement

OCR has the authority to settle any issue or case with the covered entity or business associate, regardless of any ALJ determination. *45 C.F.R. §§ 160.416*, *160.514*. Typically, in this case, the parties enter a resolution agreement requiring the respondent to perform certain obligations and make reports to OCR, usually for a period of three years. The resolution agreement may also include a requirement that the covered entity or business associate make a monetary payment, known as a resolution amount.

If OCR cannot reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, HHS may still impose penalties against the covered entity. See *HHS, Resolution Agreements and Civil Money Penalties*.

Enforcement Action, Resolution Agreement, and CMP Examples

For examples of OCR enforcement action resolution agreements and CMPs, see *HHS, Health Information Privacy: Resolution Agreements and Civil Money Penalties*. A broader list of OCR cases that identifies the HIPAA issue involved can be found at *HHS, Health Information Privacy: All Case Examples*. A summary of enforcement activity from 2014–2016 is provided below under *OCR Enforcement Activities*.

Civil Monetary Penalties for HIPAA Administrative Simplification Rule Violations

OCR can impose a penalty on a covered entity or a business associate if it determines it violated one or more administrative simplification provisions that could not be resolved by informal means. *42 U.S.C. § 1320d-5*; *45 C.F.R. § 160.402(a)*. OCR will penalize each covered entity or business associate that bears responsibility for a violation. *45 C.F.R. § 160.402(b)(1)*. The federal common law of agency explicitly applies such that entities are liable for acts or omissions of the entity's agent. *45 C.F.R. § 160.402(c)*.

Factors Affecting Penalty Amount

The amount of a CMP that OCR may impose for a HIPAA violation is subject to the limits noted in the chart below and must be determined by considering the following factors:

- Nature and extent of the violation (e.g., considering the number of individuals affected and time period over which the violation occurred)
- Nature and extent of resulting harm (including consideration of whether harm was physical, financial, reputational, or hindered the individual's health care access)
- Entity's history of HIPAA compliance (e.g., considering whether the same or similar violation has occurred previously and remediation efforts for prior noncompliance)
- Financial condition of covered entity or business associate (e.g., considering whether the entity had financial difficulties affecting its ability to comply or if penalties would jeopardize its ability to pay for or provide health care)
- Other matters as justice may require

45 C.F.R. § 160.408.

In addition, OCR may waive a penalty, in whole or part, where it determines that the penalty would be excessive relative to the violation. *45 C.F.R. § 160.412*.

CMP Limitations

Limitations on HIPAA civil penalties set a minimum and maximum amount per violation (except for the last category) and aggregate cap per calendar year (for an identical violation), based on a tiered structure depending the covered entity's or business associate's level of culpability. The dollar amounts are adjusted annually for inflation. The following chart shows penalty ranges and amounts for infractions occurring in the years 2016 through 2019:

Level of culpability	Description	2016	2017	2018/2019
No knowledge	Entity did not know—and by exercising reasonable diligence would not have known—that it violated HIPAA	$110–$55,010 per violation up to $1,650,300	$112–$55,910 per violation up to $1,677,299	$114–$57,051 per violation up to $1,711,533
Reasonable cause and no willful neglect	Violation due to reasonable cause and not willful neglect (minimum/maximum per violation)	$1,100–$55,010 per violation up to $1,650,300	$1,118–$55,910 per violation up to $1,677,299	$1,141–$57,051 per violation up to $1,711,533
Willful neglect and timely corrected	Violation due to willful neglect and corrected within 30 days after entity had knowledge of failure (or after would have had knowledge by exercising reasonable diligence)	$11,002–$55,010 per violation up to $1,650,300	$11,182– $55,910 per violation up to $1,677,299	$11,410–$57,051 per violation up to $1,711,533

Willful neglect and not timely corrected	Violation due to willful neglect but not corrected during 30-day period described above	$55,010–$1,650,300 per violation up to $1,650,300	$55,910–$1,677,299 per violation up to $1,677,299	$57,051–$1,711,533 per violation up to $1,711,533

42 U.S.C. § 1320d-5(a); *45 C.F.R. § 160.404(b)(2)*; *83 Fed. Reg. 51,369 (Oct. 11, 2018)*.

When considering potential liability, keep the following important rules in mind:

- If the entity can show that the violation was not due to willful neglect and it corrected the violation in a timely manner, there is no penalty. See "Affirmative Defenses" section above and *45 C.F.R. § 160.410(c)*. See also *42 U.S.C. § 1320d-6(b)(2)*.
- A penalty may be imposed for a violation of only a single administrative simplification violation even if the provision's requirement or prohibition is repeated in a more general form in another administrative simplification provision. *45 C.F.R. § 160.404(b)(3)*.
- For purposes of determining the number of violations and aggregation for the annual cap, OCR looks at the nature of the entity's obligation to act or not act under the relevant HIPAA provision (e.g., was an act required, was a deadline missed, or was an individual excluded?). *45 C.F.R. § 160.406*.
- Separate violations occur each day the entity remains in violation of a provision for cases of ongoing noncompliance. *45 C.F.R. § 160.406*.

OCR Enforcement Activities

From the April 2003 compliance date for the HIPAA Privacy Rule through 2018, OCR received over 186,453 HIPAA complaints and has initiated over 905 compliance reviews, resolving 96% of these cases (178,834). The compliance issues investigated the most by OCR are, in order of frequency:

- Impermissible uses and disclosures of PHI
- Lack of safeguards for PHI
- Lack of patient access to their PHI
- Lack of administrative safeguards of electronic PHI –and–
- Use or disclosure of more than the minimum necessary PHI

HHS Enforcement Highlights: Enforcement Results as of July 31, 2018.

Enforcement Results Data

The HIPAA privacy, security, and breach notification rule violations addressed by OCR fall into one of the following outcome categories:

- **Resolved after intake and review (without investigation).** The types of cases closed under this category are those where OCR lacks jurisdiction, or the complaint, referral, breach report, news report, or other instigating event will not be investigated, such as in cases where OCR determines that the organization alleged to have violated HIPAA rules is not a covered entity or business associate and/or no PHI is involved, the behavior of the organization does not implicate HIPAA rules, the complainant refuses to provide consent for his/her information to be disclosed as part of the investigation, or OCR otherwise decides not to investigate the allegations.
- **Technical assistance (without investigation).** OCR provides technical assistance to the covered entity, business associate, and complainant through early intervention by investigators located in headquarters or a regional office.

- **No violation found (after investigation).** OCR's investigation determines that there was no infraction.
- **Corrective action taken (after investigation).** OCR investigated and provided technical assistance on, and/or requires the covered entity or business associate to make changes regarding, HIPAA-related privacy and security policies, procedures, training, or safeguards. Sometimes, technical assistance is provided after investigation without requiring specific corrective action, such as where the entity has already taken corrective action during the investigation or within the 60-day window prior to notifying OCR of a breach incident. Corrective action closures include those in which OCR enters into a settlement agreement with a covered entity or business associate. To promote systemic reform that benefits the greatest number of individuals, in such cases, OCR settles for a percentage of any applicable penalties that OCR could impose and requires entities to reinvest in their enterprises to correct the underlying root causes for the noncompliance through a corrective action plan, which includes OCR monitoring.
- **Other**. These may include the following:
    - o Referring the matter to the Department of Justice for prosecution
    - o Matters where a natural disaster is involved
    - o The matter was pursued, prosecuted, and resolved by state authorities –or–
    - o The covered entity or business associate has taken steps to comply with the HIPAA rules and OCR determines enforcement resources are more effectively deployed in other cases

HHS, Health Information Privacy: Enforcement Data.

The following tables provide data for the years 2014–2016 regarding OCR's enforcement activities reflecting the categories above.

Complaints

Year	Resolved after intake and review	Technical assistance	Investigated: no violation	Investigated: corrective action taken	Total
2014	10,401	5,128	668	1,288	17,485
2015	12,634	3,817	360	730	17,541
2016	16,780	6,204	204	706	23,894

Breach Compliance Review Cases

Year	Resolved after intake and review	Investigated: no violation	Investigated: corrective action taken	Other	Total
2014	7	6	216	10	239
2015	8	9	126	5	148
2016	8	25	283	3	319

Other Compliance Review Cases

Year	Resolved after intake and review	Investigated: no violation	Investigated: corrective action taken	Other	Total
2014	0	2	27	1	30
2015	2	7	24	3	36
2016	1	3	10	1	15

Cases Resulting in CMPs or Settlements

Year	Total complaints and compliance reviews	Total cases investigated	Number of CMPs or settlements	% of complaints/compliance reviews resulting in CMP	% of cases investigated resulting in CMP or settlement

				or settlement	
2014	17,754	2,207	7	0.0394%	0.11%
2015	17,725	1,256	6	0.0339%	0.32%
2016	24,228	1,231	13	0.0537%	

HHS, Health Information Privacy: Enforcement Results by Year.

Criminal Penalties for Intentional HIPAA Violations

The U.S. Department of Justice (DOJ) has jurisdiction to enforce criminal penalties for violations of the HIPAA Administrative Simplification provisions under *42 U.S.C. § 1320d-6*. Such penalties may apply to persons who knowingly:

- Use or cause to be used a unique health identifier
- Obtain individually identifiable health information –or–
- Disclose individually identifiable health information to another person, in each case in a manner that violates HIPAA requirements

42 U.S.C. § 1320d-6(a).

According to a *DOJ memorandum*, the knowing standard used in the statute requires only that the person have knowledge of the facts that constitute the offense, not knowledge that the act is a violation of HIPAA.

Criminal penalties are:

- A fine of not more than $50,000, imprisonment of not more than one year, or both for knowing violations
- A fine not to exceed $100,000, imprisonment of not more than five years, or both if the offense is committed under false pretenses –or–
- A fine up to $250,000, imprisonment of up to 10 years, or both if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm

42 U.S.C. § 1320d-6(b).

Where an infraction results in a criminal penalty, the covered entity or business associate is not subject to an additional CMP (or liability for damages under state attorneys general enforcement).

State Attorneys General Enforcement

State attorneys general can seek injunctive relief and statutory damages (and potentially attorney's fees) for HIPAA administrative simplification rule violations if residents of that state have been adversely affected by the violation. Statutory damages are $100 per violation up to $25,000 for all violations of an identical requirement or prohibition during a calendar year, subject to adjustment by the court for mitigating factors discussed earlier. *42 U.S.C. § 1320d-6(d)*.

Liability for damages is not applicable if the violation was due to a reasonable cause and the covered entity or business associate timely corrects it. *42 U.S.C. § 1320d-6(b)(2)*.

HIPAA Compliance Audits and Best Practices for Avoiding Penalties

In March 2016, OCR published its audit protocol for conducting HIPAA audits. The protocol covers nearly every aspect to the HIPAA privacy, security, and breach notification requirements. *HHS, Health Information Privacy: Audit Protocol – Updated July 2018*.

At the same time, OCR announced that it would begin audits of covered entities and business associates for compliance with these requirements. In addition to making sure that the legal requirement is satisfied, the audit protocol often requires documentary proof of the satisfaction of HIPAA requirements. The audit protocol emphasizes the that compliance with the applicable HIPAA regulatory requirements should be documented. In conducting audits, OCR will ask to see if a mitigation plan was carried out and how the plan was implemented in situations where noncompliance has occurred. *HHS, HIPAA Privacy, Security, and Breach Notification Audit Program*.

HIPAA Compliance Best Practices

Covered entities and business associates can help avoid HIPAA violation penalties by taking the steps listed below. These best practices should also put the entity in a good position if OCR initiates a HIPAA audit of their practices.

- **Conduct an internal audit.** Engage an independent auditor with expertise in HIPAA compliance and have it conduct an audit of your existing HIPAA policies and procedures. Have the auditor develop a checklist to simplify an annual review of HIPAA compliance and to keep you apprised of new developments in the area.
- **Conduct annual self-audits following internal audit.** After obtaining an independent audit of HIPAA compliance policies and procedures, conduct internal annual self-audits. Be sure to periodically confirm that the audit review remains up-to-date with the latest HIPAA rules.
- **Adopt procedures to comply with HIPAA requirements.** If you have not already done so, review the audit protocol and adopt procedures and documentation to comply with all HIPAA administrative simplification requirements.
- **Develop HIPAA training materials for personnel handling PHI and safeguarding HIPAA security.** Develop training materials and periodically train all staff handing PHI or dealing with information systems impacting HIPAA's security rules. Maintain copies of the training material and periodically update them to reflect changes in the law and new developments in HIPAA compliance.
- **Conduct a risk assessment.** Conduct a risk assessment to determine compliance with the HIPAA security rules. HHS has an *online risk assessment tool*.
- **Review business associate agreements.** Review contracts with all third-party service providers that create, handle, transmit, or otherwise have access to the covered entity's PHI. Make sure compliant business associate agreements are in place. Pay special attention to the indemnification provisions to make sure that the employer is not required to indemnify the vendor for any liabilities resulting from the regular performance of the duties that the vendor was contracted to perform. If the contract requires such indemnification, either renegotiate the contract with the existing vendor or send out requests for proposal for vendors to bid on this service.
- **Review cybersecurity insurance policies.** Read the plan sponsor's liability insurance policies to make sure that they cover liability for cybersecurity breaches. If the liability insurance policy does not include cyber coverage, either purchase a rider or endorsement or send out requests for proposal to possible insurers to bid for purchasing such additional coverage. An insurance broker may be able to be used to assist the employer this policy review.
- **Cooperate with OCR if an investigation ensures.** If the employer is audited, cooperate with the auditor and promptly produce all requested documentation and truthfully respond to any questions.
- **Act promptly.** As soon as there is any indication that a HIPAA administrative simplification violation may have occurred, take steps immediately to assess the situation and take curative actions. Prompt action can be the difference between substantial penalties and no penalty.

End of Document