

HIPAA ENFORCEMENT GUIDE

by Daniel J. Solove



The Health Insurance Portability and Accountability Act (HIPAA) regulations govern health information maintained by various entities covered by HIPAA (“covered entities”) and other organizations that receive protected health information (PHI) from covered entities when performing functions for them. HIPAA is enforced by the Office for Civil Rights (OCR) in the Department of Health and Human Services (HHS).

Additionally, state attorneys general (AGs) may enforce HIPAA – only a few federal privacy laws can also be enforced by state AGs. Although the vast majority of HIPAA violations involve civil penalties, there can be criminal HIPAA violations, which are enforced by the Department of Justice (DOJ).



U.S. Department of Health and Human Services



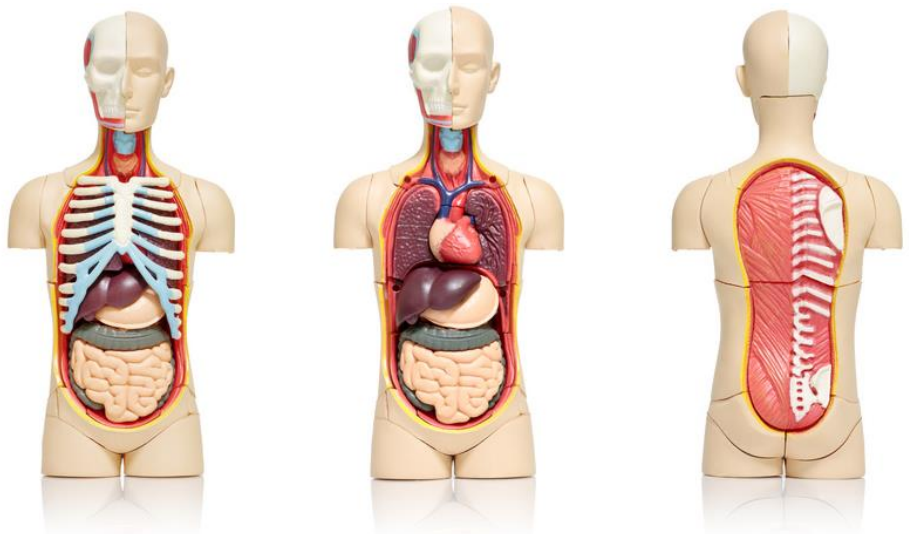
The Anatomy of a HIPAA Enforcement Action

HIPAA enforcement actions are typically initiated by a complaint. The HIPAA statute doesn’t authorize people to sue for HIPAA violations, so people’s recourse under HIPAA is to file a complaint with OCR. People can sue under state law for many of the things that would constitute HIPAA violations, as HIPAA doesn’t preempt state law, and more privacy-protective state law trumps HIPAA in those states in which it is enacted.

When OCR receives a complaint, it first evaluates whether it has jurisdiction and whether there is a possible violation. It will then launch an investigation and reach a resolution. That resolution can be a finding of no violation or of a violation. Many cases are resolved by the entity being investigated agreeing to take corrective action and sometimes agreeing to pay monetary penalties.

HIPAA enforcement actions can also be triggered when there is an incident that is reported to HHS, such as a data breach.

HIPAA enforcement now also involves auditing.



The Scope of HIPAA Enforcement

OCR can enforce HIPAA against a wide array of entities. Covered entities large and small are subject to OCR enforcement – from small doctors’ offices to large hospitals and health systems. OCR can enforce against not only private-sector entities but public sector ones as well. For example, one action was against a state’s Department of Health and Human Services.

OCR also has the ability to directly enforce HIPAA against business associates – and any subcontractors of business associates.

HIPAA enforcement thus follows PHI wherever it goes – except under special circumstances. So if a hospital provides PHI to a billing company, and the company subcontracts with another entity, OCR can enforce down the chain of custody. HIPAA thus is enforced along the chain . . . and PHI generally remains inside HIPAA’s protective bubble no matter where the hot potato is handed.

This concept of enforcement along the chain is really essential in today’s age where data can so readily be transferred and where so many entities have access to particular pieces of personal data. Unfortunately, unlike HIPAA, many other privacy laws do not allow for enforcement along the chain – the Family Educational Rights and Privacy Act (FERPA) is an example. Once education records are handed to others, the Department of Education is powerless to enforce against those entities.



The Story of HIPAA Enforcement

The story of HIPAA enforcement is a tale of two OCRs – the one before HITECH and the one after.



HIPAA Enforcement Before HITECH

Initially, between 2003 and 2008, HIPAA enforcement would best be characterized as a cooperative model. OCR would work with institutions to help them sin no more. The goal was not penal, but being helpful. The saying “I’m from the government, and I want to help” really applied here.

By 2008, more than 33,000 complaints had been filed with OCR. About 8000 of those were investigated, leading to 5600 instances where entities took corrective action. No fines were ever issued. Critics called HIPAA’s enforcement toothless.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act seriously ratcheted up the penalties. The fines for HIPAA violations were raised dramatically -- up to more than \$1.5 million for a violation in certain circumstances. The HITECH Act added a breach notification requirement and it mandated that HHS conduct compliance audits. Congress made clear that HIPAA enforcement should have more teeth – and that OCR should be issuing some fines.

The HITECH Act significantly renovated HIPAA. In my opinion, HITECH was one of the best set of improvements to a privacy law that Congress has ever made.

In 2013, HHS issued the Omnibus Final Rule implementing HITECH Act changes in HIPAA. But its enforcement approach changed earlier, right after the HITECH Act.

HIPAA Enforcement After HITECH

Since 2013, we are seeing HIPAA enforcement resolutions that include fines. But even today, most HIPAA enforcement resolutions “simply spell out corrective action plans or offer technical assistance.”

There have now been more than 60 cases involving financial payments or a civil monetary penalty.



Enforcement Statistics

The story for HIPAA case resolutions is that they have been generally increasing throughout the years. Starting in 2008, there have been between 8,000 to 10,000 resolutions. There was a huge spike in the number in 2013 after the Omnibus Final Rule, an increase from 9,408 in 2012 to 14,300 in 2013. In 2016, that number surpassed 24,000 cases.

Most cases still get resolved without a monetary penalty. But the number of cases with monetary penalties has been increasing, and the penalties are quite steep.



Resolution Agreements

When a civil monetary penalty is involved, HHS will enter into a resolution agreement with the entity. A resolution agreement includes:

- a financial penalty
- a corrective action plan (CAP) that often involves entities improving their policies and procedures, training, risk analyses, and security practices
- a reporting requirement, typically ranging from 1 to 3 years



How Painful Is HIPAA's Sting?

The penalties as part of the resolution agreements are quite steep.

2012

Total: \$4.8 million
Range: \$50,000 to \$1.7 million
Average: \$970,000

2015

Total: \$6.19 million
Range: \$125,000 to \$3.5 million
Average: \$1.03 million

2018

Total: \$25.64 million
Range: \$100,000 to \$16 million
Average: \$3.2 million

2013

Total: \$3.49 million
Range: \$150,000 to \$1.7 million
Average: \$678,656

2016

Total: \$23.48 million
Range: \$25,000 to \$5.5 million
Average: \$1.56 million

2014

Total: \$7.94 million
Range: \$150,000 to \$3.3 million
Average: \$1.13 million

2017

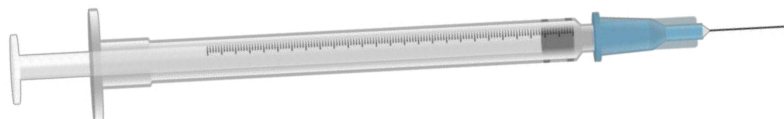
Total: \$19.39 million
Range: \$31,000 to \$5.5 million
Average: \$1.94 million

The Many Flavors of Resolution Agreements

The OCR resolution agreements appear to be deliberately eclectic, involving institutions large and small, as well as many different types of incidents. They represent a nice cross-section of different types of HIPAA violations. To a HIPAA wonk like me, reading them is akin to going into a gelato store and being able to taste all the flavors. (Having done both, I would opt for the gelato store if you had a choice.)

Is Harm Needed for a Penalty?

Harm isn't required for there to be a monetary penalty. In one case, PHI was left in boxes unattended in a driveway to a house. But there were no allegations that any unauthorized individual accessed the PHI or took the records. There were no allegations that any PHI was lost. Nevertheless, the monetary penalty was \$800,000.



HIPAA Enforcement Cases with Monetary Penalties

Case	Date	HIPAA Issues	Penalty
Providence Health and Services	7/16/08	Unencrypted laptops and other devices stolen	\$100,000
CVS Pharmacy	1/15/09	Improper disposal of documents containing PHI Failure to properly train employees	\$2.25 million
Rite Aid Corp.	6/7/10	Improper disposal of documents containing PHI Failure to properly train employees	\$1 million
Management Services Organization Washington, Inc.	12/13/10	Unauthorized use of PHI in marketing materials	\$35,000
Cignet Health	2/4/11	Denied access to patient's own medical records	\$4.3 million
General Hospital Corp. and Massachusetts General Physicians Organization, Inc.	2/14/11	Employee left documents containing PHI on the subway	\$1 million
University of California at Los Angeles Health System	7/6/11	Unauthorized access of PHI Failure to properly train employees	\$865,000
Blue Cross Blue Shield of Tennessee	3/9/12	Unencrypted computer hard drives stolen	\$1.5 million
Phoenix Cardiac Surgery	4/11/12	PHI inadvertently made available over the internet Failure to properly train employees	\$100,000
Alaska Department of Health and Social Services	6/25/12	Unencrypted device stolen Failure to properly train employees	\$1.7 million
Massachusetts Eye and Ear Infirmary	9/17/12	Unencrypted laptop stolen	\$1.5 million
Hospice of Northern Idaho	12/17/12	Unencrypted laptop stolen	\$50,000
Idaho State University	5/13/13	Disabled firewalls caused breach of ePHI	\$400,000
Shasta Regional Medical Center	6/6/13	Details of patient's medical services released to media without authorization	\$275,000
WellPoint, Inc.	7/8/13	PHI inadvertently made available over the internet	\$1.7 million
Affinity Health Plan	8/7/13	PHI inadvertently disclosed by failure to erase hard drive on leased device	\$1.2 million
Adult & Pediatric Dermatology	12/24/13	Unencrypted device stolen Lack of written policies and employee training	\$150,000
Skagit County, Washington	3/6/14	PHI inadvertently made available on public server Failure to notify individuals whose PHI had been compromised	\$215,000
QCA Health Plan, Inc.	4/14/14	Unencrypted laptop stolen	\$250,000
Concentra Health Services	4/21/14	Unencrypted laptop stolen	\$1.725 million
Columbia University	5/7/14	PHI inadvertently made available to Internet search engines	\$1.5 million
New York Presbyterian Hospital	5/7/14	PHI inadvertently made available to Internet search engines	\$3.3 million
Parkview Health System, Inc.	6/23/14	Failure to appropriately safeguard PHI	\$800,000
Beth Israel Deaconess Medical Center	11/20/14	Unencrypted laptop stolen	\$100,000
Anchorage Community Mental Health Services	12/2/14	Malware infection led to unauthorized disclosure of PHI	\$150,000
Boston Children's Hospital	12/19/14	Unencrypted laptop stolen	\$40,000
Cornell Prescription Pharmacy	4/22/15	Improper disposal of documents containing PHI Lack of written policies and employee training	\$125,000
St. Elizabeth's Medical Center	6/10/15	File-sharing application risked exposing PHI Unsecured PHI on former employee's laptop breached	\$218,400
Cancer Care Group, P.C.	8/31/15	Unencrypted device and computer stolen	\$750,000
Lahey Hospital and Medical Center	11/24/15	Laptop stolen from unsecured room	\$850,000

Case	Date	HIPAA Issues	Penalty
Triple-S Management Corporation	11/30/15	Failure to safeguard PHI Failure to execute proper business associate agreement	\$3.5 million
University of Washington Medicine	12/14/15	Malware infection led to unauthorized disclosure of PHI	\$750,000
Lincare, Inc.	2/3/16	Unencrypted PHI taken offsite and abandoned	\$239,800
Complete P.T., Pool & Land Physical Therapy, Inc.,	2/16/16	Unauthorized use of PHI in marketing materials	\$25,00
North Memorial Health Care	3/16/16	Unencrypted laptop stolen Failure to execute proper business associate agreement	\$1.55 million
Feinstein Institute for Medical Research,	3/17/16	Unencrypted laptop stolen	\$3.9 million
Raleigh Orthopaedic Clinic,	4/14/16	Failure to execute proper business associate agreement	\$750,000
New York & Presbyterian Hospital	4/19/16	Unauthorized disclosure and failure to safeguard PHI to film crew	\$2.2 million
Catholic Health Care Services of the Archdiocese of Philadelphia	6/29/16	Unencrypted phone stolen	\$650,000
Univ. of Miss. Med. Ctr.	7/7/16	Encrypted laptop stolen PHI vulnerable to unauthorized access on wireless network Failure to notify individuals affected by data breach	\$2.75 million
Oregon Health & Science University	7/18/16	Two unencrypted laptops and 1 unencrypted thumb drive stolen Failure to execute proper business associate agreement	\$2.7 million
Advocate Health Care Network	8/4/16	Unencrypted laptop stolen Failure to execute proper business associate agreement	\$5.55 million
Care New England Health System	9/23/16	Lost unencrypted backup tapes Outdated business associate agreement	\$400,000
St. Joseph Health,	10/17/16	Unauthorized disclosure and compromised PHI	\$2.14 million
University of Massachusetts	11/22/16	Malware infection led to unauthorized disclosure of PHI	\$650,000
Presence Health	1/9/17	Lack of timely breach notification	\$475,00
MAPFRE Life Insurance Company of Puerto Rico	1/18/17	Unsecured USB device stolen Failure to implement effective risk assessment and management	\$2.2 million
Children's Medical Center of Dallas	2/1/17	Unsecured phone and laptop stolen Failure to implement effective risk assessment and management	\$3.2 million
Memorial Healthcare System	2/16/17	Improper access and disclosure of PHI Failure to implement audit controls and review audit logs of access to PHI	\$5.5 million
Metro Community Provider Network (MCPN)	4/12/17	Phishing incident led to unauthorized disclosure of PHI Failure to implement effective risk assessment and management	\$400,000
The Center for Children's Digestive Health (CCDH)	4/20/17	Failure to execute proper business associate agreement	\$31,000
CardioNet	4/24/17	Unencrypted laptop stolen Insufficient risk analysis and risk management processes Noncompliance with the HIPAA Privacy and Security Rules	\$2.5 million
Memorial Hermann Health System (MHHS)	5/10/17	Impermissible disclosure of patient's PHI in press release	\$2.4 million
St. Luke's-Roosevelt Hospital Center Inc.	5/23/17	Staff member faxed patient's PHI to employer rather than patient's requested personal P.O. box	\$387,200
21st Century Oncology, Inc. (21CO)	12/28/17	Failure to conduct assessment of the potential risks and vulnerabilities of PHI Failure to implement security measures Failure to implement procedures to regularly review records of information system activity Disclosed PHI to third party vendors without a written business associate agreement	\$2.3 million

Case	Date	HIPAA Issues	Penalty
Fresenius Medical Care North America	02/01/18	Failure to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI. Disclosed the ePHI of patients by providing unauthorized access for a purpose not permitted by the Privacy Rule	\$3.5 million
Filefax, Inc.	02/13/18	Filefax impermissibly disclosed the PHI of 2,150 individuals either by leaving the PHI in an unlocked truck in the Filefax parking lot, or by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unsecured outside the Filefax facility	\$100,000
The University of Texas MD Anderson Cancer Center	06/18/18	Failure to encrypt inventory of electronic devices containing ePHI	\$4.3 million
Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH)	09/20/18	Compromised patients' PHI by inviting film crews on premises to film an ABC television network documentary series without first obtaining authorization from patients	\$999,000
Anthem, Inc.	10/15/18	Hackers gained access to Anthem's computer system when one employee at an Anthem subsidiary responded to a spear phishing email. Hackers stole ePHI of nearly 79 million people. Anthem failed to conduct risk analysis, had insufficient procedures to regularly review information system activity, failed to respond to suspected or known security incidents, and failed to implement adequate minimum access controls.	\$16 million
Allergy Associates of Hartford, P.C.	11/26/18	Impermissibly disclosed a patient's protected health information to a reporter. Failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media.	\$125,000
Advanced Care Hospitalists PL (ACH)	12/4/18	Failed to enter into a business associate agreement with the individual providing medical billing services to ACH, as required by HIPAA. Failed to adopt any policy requiring business associate agreements until April 2014. Although in operation since 2005, the company had not conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014.	\$500,000
Pagosa Springs Medical Center (PSMC)	12/11/18	Failed to remove former employee's access to web-based scheduling calendar, which contained PHI of 557 patients. Also failed to obtain BAA with calendar company (Google) and therefore, disclosed PHI to them as well.	\$111,400
Cottage Health	12/12/18	Two breaches of unsecured electronic protected health information (ePHI) affecting over 62,500 individuals, one in December 2013 and another in December 2015. Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the ePHI; Failed to implement security measures; Failed to perform periodic technical and non-technical evaluations; and Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.	\$3 million

State HIPAA Enforcement

In addition to increasing penalties and mandating audits, HITECH also permitted state attorneys general to bring enforcement actions for HIPAA violations at the pre-HITECH penalty levels. Of the actions brought, all state attorneys general have also relied on state data protection laws.



The Big Picture of HIPAA Enforcement

Let's step back and look at the big picture of HIPAA enforcement. Recently, at the end of 2013, the total number of HIPAA complaints received by OCR since 2003 exceeded 100,000. By the end of 2016, the number surpassed 150,000.

Since 2009, there have been more than 1000 data breaches involving 500 or more people that have been listed on the HHS "wall of shame" website. Of these OCR completed 751 investigations.

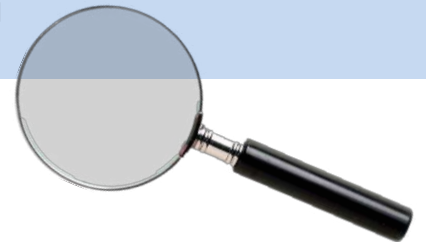
One of the great things about HHS enforcement is that HHS maintains some of the most comprehensive statistics and information on its website. Other agencies only report a fraction of what HHS reports. And some barely have anything on their websites at all.

One interesting difference between HHS and the FTC is that HHS reports on the cases it investigates, whereas the FTC often keeps it a secret when it conducts an investigation and resolves not to take action.

The Most Investigated Compliance Issues

According to HHS, the compliance issues most investigated include:

- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
- Lack of patient access to PHI
- Uses or disclosures of more than the minimum necessary PHI
- Lack of administrative safeguards of ePHI



Analysis and Takeaways

HIPAA enforcement has teeth.

HIPAA enforcement used to be toothless; now, post-HITECH, it has some teeth and significant fines have been issued. HITECH really strengthened HIPAA in many ways. This is not your grandfather's HIPAA anymore – it's much more powerful.

HIPAA enforcement is increasing.

The number of cases with corrective action taken has risen steadily throughout the years. And HIPAA enforcement activity is increasing, with larger fines being issued.

HIPAA can be enforced all along the chain of custody of PHI.

HIPAA allows for HHS enforcement along the chain of custody of PHI. This is a really essential protection, as these days, it is so common for PHI to circulate among various entities.

State AGs can join in on the enforcement fun.

HIPAA allows state AGs to enforce, though not many have availed themselves of this power.

Incidents and breaches are often the tip of the iceberg.

Although an incident might spark an investigation, the resolution agreements show that the incident is just the tip of the iceberg. There are other HIPAA compliance shortcomings that OCR will typically find. Turn over the stone, and you'll often find more than one bug crawling underneath.



Enforcement actions with monetary penalties have recurring themes.

Reading the resolution agreements reveals some recurring themes about what issues OCR will single out for monetary penalties:

1. Unencrypted data on portable devices
2. Failure to conduct risk assessments
3. Failure to monitor and control access to PHI
4. Failure to have good workforce training





About the Author

Professor **Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world's leading experts in privacy law, Solove has taught privacy and security law every year since 2000, has published 10 books and more than 50 articles, including the leading textbook on privacy law and a short guidebook on the subject.



Professor Solove has spoken at hundreds of universities, federal agencies, and other organizations. He has given keynote addresses at many conferences, including one organized by the U.S. Department of Health and Human Services.

He has [more than 1 million followers](#) on LinkedIn.

Professor Solove organizes many events per year, including the [Privacy+Security Forum](#) and the [International Privacy+Security Forum](#).

About TeachPrivacy

TeachPrivacy was founded by Professor Daniel J. Solove. He is deeply involved in the creation of all training programs because he believes that training works best when made by subject-matter experts and by people with extensive teaching experience.



TeachPrivacy has a library of more than 100 training courses that cover a wide array of privacy and security topics including HIPAA, FERPA, PCI, phishing, social engineering, and many others.