

Policy Analysis HIPPA

Max Khamphavong

CYSE 425, Old Dominion University

Sept 12, 2025

The Health Insurance Portability and Accountability Act, HIPPA, is one of the most fundamental and important policies that the United States government enforces to protect businesses and consumer health data. While HIPPA is most seen and viewed in the medical sectors and often discussed in hospital or doctors' offices the regulation is used almost universally. I choose HIPPA as my topic because it relates to what I do as my full-time job doing data analysis and processing from my company.

The company I work is called Preferred Direct Marketing Services and it as a commercial printing/marketing firm. Our largest client happens to be Amerigroup, also known as Anthem, which is one of the largest health insurers in the United States. Here I work with a large file containing PHI (Private Health Information). The files are sent between the Anthem and Preferred Direct via encrypted FTP servers. Next, I then process the data through a client called BCC Mail Manager which organizes the data to comply with HIPPA and USPS regulations. Finally, once the data has been processed the formatted, I then merge the data through software called Ulro which handles merging with our graphics department. If we do not follow proper HIPPA protocols the company can be fined over one hundred thousand dollars. That being said it is important we look the data and follow the proper safety measures to protect and uphold the data standards.

HIPPA was enacted back in 1996, and its core purpose was to protect people by making health insurance portable so workers would not lose any coverage if they changed jobs. With rise of the general consumer internet, it was only a matter of time before regulations and rules needed to be set over PHI data. Over time HIPPA has progressed to become what we know today as the

fundamental laws and regulations for privacy and security. HIPPA contains two large rules, the first being Privacy Rules and the second being Security Rule. These lay out how health data should be properly stored, transferred, and protected. HIPPA also ensures the CIA Triad which stands for continentality, integrity, and availability which happens to be a core fact in cybersecurity. These frameworks today act as the grounds for health systems in the United States to protect everyone.

Although HIPPA is not the only policy applied to keep data safe it is one of the largest most influence policies to business and health sectors. In 2009 the US government passed the Economic and Clinical Health ACT (HITECH) built on HIPPA fundamentals to require organizations to announce data breaches or major security issues that can impact the individuals. Over in the European Union they have something like HIPPA which is called the European General Data Protection Regulation (GDPR). These regulation acts protect people's data on a broader scale, but overall, both show the shift to individual rights and data protections. Today we see HIPPA adjacent regulations applied in our day to day tasks. Business's must do regular data logging and audits to ensure it following the CIA Triad. Further steps to increase security measures such as two factor authentication, encryptions, and vendor oversight. Something I thought that was a cool fact was that my job also uses DUO mobile which here at ODU we use when logging into applications like our portals.

On a national level HIPPA is one of the core baselines for compliance and protections. They complement alongside the NIST SCF and overall United States National Cybersecurity strategies by enforcing these rules that also carry civil penalties. I choose HIPPA because of my job and how everything I do falls with those compliance and I have a sort of relatability to the topic. I also am to follow the career path to become a GRC Analysis up in the Northeast one day.

This means will be working alongside many policies HIPPA being a large example. Thanks to my job and experience, I believe I will most likely enter the data side of health sectors or IT as a long-term carrier choice.

Citations

Steven Char, Kenneth Prager, Lydia Dugdale, Katherine Fischkoff, Surgeon Perspectives on Daily Presentation of Ethical Dilemmas: A Qualitative Study, Journal of the American College of Surgeons, 237, 5, (751-761), (2023).

<https://doi.org/10.1097/XCS.0000000000000802>

Nass, S. J. (1970). Introduction. Retrieved from <https://www.ncbi.nlm.nih.gov/books/NBK9576/>

Suzy A. Buckovich, Helga E. Rippen, Michael J. Rozen, Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information, Journal of the American Medical Informatics Association, Volume 6, Issue 2, March 1999, Pages 122–133,

<https://doi.org/10.1136/jamia.1999.0060122>

Ness RB, Joint Policy Committee, Societies of Epidemiology FT. Influence of the HIPAA Privacy Rule on Health Research. JAMA. 2007;298(18):2164–2170. doi:

<https://doi.org/10.1001/jama.298.18.2164>

Seema Belani, Georgina C Tiarks, Neil Mookerjee, Vijay Rajput, “I Agree to Disagree”: Comparative Ethical and Legal Analysis of Big Data and Genomics for Privacy, Consent, and Ownership, Cureus, (2021).

<https://doi.org/10.7759/cureus.18736>

