HIPAA COMPLIANCE - BALANCING PRIVACY, PROTECTION, AND PORTABILITY

THE COMMAND POST

SERIES - 3 / ARTICLE - 3

SEPTEMBER 07, 2022

By **Jeffrey Brochin, Esq.**

GreenPoint> Law&Compliance

william.anderson@greenpointglobal.com | pranav.menon@greenpointglobal.com

International Corporate Center, 555 Theodore Fremd Avenue, Suite A102 Rye, NY 10580

www.greenpointlegal.com

We all expect that our personal health information will be kept strictly confidential, right? However, there is a difference between confidentiality and privacy. But what is it? In today's technologically advanced health care system, your medical information is likely 'shared' by no less than a minimum of 20 different information handlers, from doctors to nurses, various technicians, insurance providers, claims processors, medical coders, ambulance drivers, and even health care volunteers. Yet, despite this widespread—and even global—sharing of your most intimate medical details, the patient's right to have it all kept private and confidential must be respected and maintained.

Why is Portability Regulated?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was originally promulgated to protect patients' rights and confidentiality in the course of moving one's health insurance from one employer to another, and to ensure that the portability of one's coverage would be a seamless and uninterrupted process. Furthermore, the Act was intended to protect the confidentiality of a patient's Protected Health Information (PHI) as the patient, by necessity, shared that information with a variety of healthcare providers.

Who is a Covered Entity?

The privacy and data security provisions in HIPAA apply to 'covered entities', defined as any healthcare organization (including a health plan) that interacts with confidential medical information in electronic form. By extension, the definition applies to any and all members of such an organization's staff, regardless of whether they are strictly medical personnel, or pharmacists, administrators, clerks, maintenance workers, or even food service workers, and, volunteers, such as 'candy stripers', assisting under a facility's direct supervision.

Businesses Beyond Medical Providers

In 2009, the Obama Administration passed the Health Information Technology for Economic and Clinical Health (HITECH) Act to encourage the adoption of health information technology, and specifically, the use of Electronic Health Records (EHR) by healthcare providers. Subsequently, in the era of cross-border exchange of data being commonplace, independent contractors and various auxiliary service providers also came under HIPAA regulation and were subject to compliance with its security provisions. Outsourced laboratory services, overseas radiologists hired to review X-rays and other diagnostic imaging results, outsourced medical coding staff, and medical records storage managers, who are all deemed 'Business Associates' as per HIPAA's 2013 revisions, and subject to HIPAA's privacy and security requirements.

The outsourcing of PHI data is a particular area of concern given the fact that some of the largest breaches of PHI security reported to the Department of Health and Human Services (HHS) have occurred while medical data was being processed by or transferred to or from such outsourced Business Associates.

THE HITECH ACT ALSO ADDRESSES THIS WITH ITS BREACH NOTIFICATION REQUIREMENTS, SPECIFYING WHEN BREACHES OF UNSECURED HEALTH INFORMATION MUST BE REPORTED TO HHS.

Understanding Privacy and Confidentiality

Although the terms 'privacy' and 'confidentiality' may often be confused or used interchangeably, HIPAA makes a distinction between the two - privacy is the patient's right to determine to whom, when, and how PHI will be disclosed. While confidentiality is the PHI handler's obligation not to disclose or expose such PHI without authorization.

As required by HIPAA, healthcare organizations have an already-prepared 'Notice of Privacy Practices' governing how patient information will be protected, what type of information may be shared and under what circumstances. Typically, the organization is permitted to share or disclose patient information as necessary for medical care or treatment, but also, to apply for payment from a health plan and in order to comply with mandatory regulatory reporting and disclosure. However, the sharing of patient information for marketing purposes is prohibited by HIPAA without patient authorization.

Penalties for HIPAA Non-compliance

In the event of a HIPAA violation by a covered entity, penalties may be administered by HHS's Office for Civil Rights (OCR), or by state attorneys general. A HIPAA violation may be deemed unintentional if, for example, more than necessary PHI has been disclosed, thereby violating the 'minimum necessary information' standard (disclosed PHI must be limited in scope to the minimum necessary to achieve the disclosure purpose). An example of a deliberate violation would be the unnecessary delay in issuing breach notification letters to patients and exceeding the maximum timeframe of 60 days following the discovery of a breach to issue notifications. Many HIPAA violations result from negligence, such as not performing a risk assessment, which is a frequent HIPAA violation. Understandably, the penalties imposed for an unintentional HIPAA violation will be at a lower rate than for willful violations.

HIPAA uses a tiered structure for imposing penalties, which are designated as:

- Tier 1 - A violation that the covered entity was unaware of and could not have realistically avoided
- Tier 2 - A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care
- Tier 3 - A violation suffered as a direct result of 'willful neglect' of HIPAA Rules,
- Tier 4 - A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

Civil money penalties have corresponding penalty tiers recited in the HITECH Act of:

- Tier 1 - Minimum fine of $100 per violation up to $50,000
- Tier 2 - Minimum fine of $1,000 per violation up to $50,000
- Tier 3 - Minimum fine of $10,000 per violation up to $50,000
- Tier 4 - Minimum fine of $50,000 per violation

However, in the event of a finding of severe negligence or willfulness, a civil money penalty can reach a maximum of $1.5 million per violation.

Conclusions

Although HIPAA started out as a statute to ease the portability of health insurance coverage for employees, Covered Entities and their Business Associates must be keenly mindful of the PHI protection and privacy aspects that have evolved into an absolute concern for the healthcare industry as a whole. Considering the regulatory liability and burdensome financial penalties, all businesses subject to the law should always keep HIPAA as the core of their compliance initiatives.

Executive Summary

1. The Issue

How to protect a patient's right to privacy under HIPAA when dealing with enormous volumes of PHI on a daily basis?

2. The Gravamen

A thorough and in-depth knowledge of the ins and outs of HIPAA compliance is essential for any healthcare organization in order to avoid non-compliance, be it by way of unintentional negligence or willful non-compliance.

3. The Path Forward

Professional training of staff, enterprise governance guidelines, and ongoing risk assessment must be adopted in order to stay compliant with HIPAA, HITECH, and related statutes and regulations.

Action Items:

1 Risk Management Assessment:

Have a Risk Management Assessment conducted in order to identify potential areas of non-compliance whether by medical personnel or administrative/clerical employees, and, require the same of any vendors your organization outsources their data processing and data management work to.

2 Risk Framework:

Once exposures and risks are analyzed, formulate a Risk Framework under which monitoring, reporting, and corrective measures will be taken as compliance and non-compliance. The Framework must designate who in the hierarchy or your organization has primary responsibility for these functions (typically a Compliance Officer) and how the Framework policies will be disseminated to all divisions within your organization down to the individual employee.

3 Regular Review:

Your Risk Assessment is not a one-off task, but rather must be built into your operations as an ongoing process. Your Framework must be regularly updated to reflect the findings of your Assessments.

4 PHI Security and Access:

Ensure that PHI security measures are up to date, and, any breaches—no matter how seemingly insignificant—are treated with the utmost seriousness, and, importantly, are disclosed to regulators where mandated.

Further Readings

1. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
2. https://lms.rn.com/getpdf.php/1808.pdf
3. https://www.cleardata.com/hipaa-security-rule-standards-and-implementation-specifications/
4. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
5. https://www.hipaajournal.com/what-is-the-hitech-act/
6. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Jeffrey Brochin, Esq.

GREENPOINT STAFF COUNSEL
AND CONTENT EDITOR

After receiving his Juris Doctor degree from The John Marshall Law School in Chicago, Mr. Brochin served as an Administrative Law Judge with the Illinois Department of Labor for six years where he presided over cases dealing with job separation issues and matters pertaining to contested Unemployment Insurance claims. He also co-wrote the agency's administrative rules, and periodically served as a 'ghost writer' for Board of Review decisions. Following that position, he was Director of Development for a Chicago-area non-profit college where he was responsible for High Net Worth donations to the institution. For the next eighteen years he practiced as a solo practitioner attorney with an emphasis in the fields of Real Estate law and Commercial Contracts transactions, and was an agent for several national title insurance agencies.

In 2003 he was recruited to head up a U.S. title insurance research office in Israel, a position he held for four years, and between 2007-2017 he participated in litigation support for several high-profile cases. He has taught Business Law as a faculty member of the Jerusalem College of Technology, and has authored a wide variety of legal White Papers and timely legal articles as a professional legal content writer for GPL clients. Separate from his legal writing, he has co-authored academic articles on Middle East security topics that have been published in peer-reviewed publications.

William H. Anderson, Esq.

MANAGING DIRECTOR AND HEAD OF
FINANCIAL PRODUCTS AND SERVICES

William Anderson is Managing Director and Head of Law & Compliance. He leads the GreenPoint practice in providing regulatory, legal, and technology solutions to law firms, legal publishers, and in-house law departments around the world, overseeing our team of experienced US attorneys and data and technology experts. Will has over 25 years' experience working with corporations to improve the management of their legal and corporate compliance functions. Will began his legal career as a litigator with a predecessor firm to Drinker, Biddle LLP. He then served as in-house counsel to Andersen Consulting LLP, managing risk and working with outside counsel on active litigation involving the firm.

Will has leveraged his legal experience interpreting regulations and appearing before federal (DOJ, SEC, FTC) and state agencies (NYAG) to oversee research and other areas at Bear Stearns. In this capacity, he counseled analysts on regulatory risk and evolving compliance requirements. Will also consulted on the development of a proprietary tool to ensure effective documentation of compliance clearance of research reports. Will then went on to work in product development and content creation for a global online compliance development firm pioneering the dynamic updating of regulated firms' policies and procedures from online updates and resources. Will holds a Juris Doctorate with High Honors from the Washington University School of Law in Saint Louis and is admitted to state and federal bars. He lives in Pawling, NY, with his wife and daughter.

Sanjay Sharma, PhD
FOUNDER AND CHAIRMAN

Pranav Menon, Esq.
LEGAL RECRUITMENT
MANAGER AND DATA
PRIVACY SPECIALIST – LAW
& COMPLIANCE | GPESR

GreenPoint> Law&Compliance

About GreenPoint Law & Compliance

- GreenPoint Global was founded in 2001 and since that time has faithfully served an expanding roster of clients. GreenPoint leverages a unique combination of US-trained attorneys and proprietary technology to deliver a unique offering of skill and flexibility to meet client needs.
- Our core team of experienced US attorneys is based in Israel and works US hours. The breadth of experience of our attorneys ensures high-quality, cost-effective results across a wide range of legal, compliance, and regulatory matters.
- GreenPoint's methodology and proven track record of achieving client objectives has resulted in a broad base of clients in the United States, ranging from Fortune 500 insurance companies to solo practitioners, law firms, in-house law departments, and legal publishers. GreenPoint attorneys are selectively recruited and deployed based on possessing demonstrable subject matter expertise covering a broad spectrum of substantive US laws and regulations. The work product of our attorneys is thoroughly vetted internally before delivery to client. Adherence to quality, value and flexibility is at the core of our foundation.

GreenPoint> Global

About GreenPoint Global

- GreenPoint Global provides litigation support, finance and technology solutions to insurers, law firms, banks, and in-house law departments through our subject matter experts and process specialists.
- Founded in 2001 and headquartered in Rye, New York, GreenPoint has grown to over 500 employees with a global footprint. We have a stable and growing client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. Our production and management teams are located in the US, India, and Israel with access to deep pools of subject matter experts. Our greatest strength is our employee-base of experienced lawyers, paralegals, process specialists, financial analysts, and software developers. We have leading edge software development capabilities with over 50 professionals on staff, working on internal and client projects.
- GreenPoint is certified by the TÜV SÜD (South Asia) for the highest standards of Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013). GreenPoint is certified as a Minority and Woman Owned Business Enterprise (MWBE) by New York City and a Minority Owned Business Enterprise (MBE) by the State of New York. GreenPoint complies with all federal and state contracting requirements. GreenPoint is owned by its founders and principals and is debt free. For comprehensive information on our services and products under Law & Compliance and Finance, please visit our subsidiary websites through the division's menu.