MHS

Beyond Assessments

Data Stewardship

In a world where every company is a data company, good data stewardship should be a fundamental organizational value since protecting data is a responsibility that lies with every person within the organization.

MHS is a trusted, global neuroscience and bioinformatics company whose purpose is to provide data-driven insights that predict and improve individual and organizational success. By the very nature of what we do, we are stewards of the personal and confidential information our customers provide. We require data to understand individual and organizational behavior, arrive at predictions, and develop effective interventions. As such, we must have a well-articulated and easy-to-follow framework for trust that governs how we engage with others and interact with the data we are entrusted with. We created the MHS Trust Framework to articulate and share our commitment to trusted relationships with our clients, partners, industry regulators, and the users of our measurement and test systems.

The MHS Trust Framework has four pillars: Ethics, Stewardship, Transparency, and Accountability. This paper delves deeper into the second of the four pillars in the MHS Trust Framework, Stewardship, focusing on Data Stewardship.

2023

The Miriam-Webster dictionary defines stewardship as:

"The careful and responsible management of something entrusted to one's care."

Applying this definition, we can think of data stewardship as "the careful and responsible management of data entrusted to one's care." It's important to emphasize that this data is entrusted to us for utilization rather than being originally our own.

As **stewards** of confidential and sensitive data, we will ensure that the intention, method (process and practice), and outcome(s) of each data use is always transparent in intent and understood and approved by all parties. Further, we will abide by the laws of each country we do business in, meeting the intent and the letter of each country's data frameworks. Where national laws of origin, processes, and transactions vary, we will work to the most stringent of options to ensure clear and consistent use of data in all cases.

Data stewardship is the encompassing responsibility we have to our customers and their customers to carefully and responsibly manage all data that has been entrusted to us. This responsibility covers all aspects of data stewardship - security, privacy, processing, and administration. In cases where original or derived data with personally identifiable elements is subsequently repackaged and sold, data stewardship would also include responsible data monetization practices.

Before I go any further, let me be clear: MHS does not and will never sell personally identifiable data. However, failure to specifically include the concept of data monetization in a discussion on data stewardship would be an omission in and of itself.

Let's delve deeper into these concepts, starting with data security and privacy. These two concepts are tightly combined and intertwined. Simply put, you can't have data privacy without data security.

Data Security

In a traditional paper and pencil environment, ensuring data security involves storing completed assessments in a secure filing cabinet with limited access. Consequently, the data remains secure if access is controlled and kept private. Expanding this concept into the digital sphere, if the data resides on a password-protected laptop, an encrypted hard drive, or a secure cloud server, and access is similarly restricted, both privacy and security are upheld.

In the context of data security practices, one should also assess the storage methods and locations for data and the policies and procedures employed by the organization with whom the data is being shared. It is crucial to understand their efforts to mitigate data breaches and unauthorized access.

While cyber security attacks by hackers make great headlines, most examples of data security breaches ultimately boil down to subpar decision-making by individuals or inadequate corporate oversight. Facebook garnered attention in the news when it was revealed that personal passwords had been unintentionally exposed for an extended period, stored in plain text within a database accessible to numerous Facebook employees. This incident serves as an illustration of lapses in human judgment, serving as a reminder that common sense is regrettably not always as prevalent as it should be.

Data Privacy

Data privacy is a multifaceted issue. Even if I possess the most highly secure data, there's still the possibility of using that data in a manner that infringes upon privacy. Consider how often you've been in public spaces like coffee shops, airport lounges, or airplanes, and you can inadvertently glimpse the screens, files, or documents of individuals working nearby. While the data may be securely stored, its privacy during use is not assured. When it's possible to trace data back to its origin, the potential for privacy breaches becomes a concern.

Several recent high-profile examples of data privacy issues include a defect in Apple's FaceTime Messenger that allowed a third party to listen in on the microphone of a party who hadn't accepted a conversation and Amazon Alexa devices that were sharing conversation fragments with unauthorized parties. Most people also weren't aware that Amazon Alexa devices share audio with third parties without permission for training purposes.

Data Processing

Data processing relates to collecting, transferring, and enriching activities such as scoring, reporting, and general data analysis. Processing responsibilities were brought to the forefront of management's attention through the introduction of the GDPR legislation.

If, for example, you send a wire transfer overseas, personal information (your name or account number) is transferred and processed by your bank and by the bank of the individual receiving the transfer. Ensuring that this data is safe throughout this transaction is exceedingly important and highlights data processing responsibilities.

Data Monetization

Data monetization is a highly charged issue. Most of us are unaware of how extensively organizations monetize our personal information. Few of us take the time to read the terms and conditions associated with websites, subscription services, or applications we use. Not to mention, it can be difficult to read an organization's legal terms and try to make sense of it. Yet, how many times are we surprised when searching for something on Amazon or a search engine, we receive advertisements for that very same product or a related item the next time we open our favorite websites? Amazon, search engines, and product review sites all use your search history within their website and across affiliated websites to create and sell targeted advertising to third parties for placement on your most-visited websites. This activity is carried out in real-time by algorithms and artificial intelligence, using the best and most currently available data about your wants, needs, and concerns to arrive at an offer you may be willing to pursue.

We are all Data Stewards – *The question is how responsible are we in this role?*

Every aspect of data stewardship deserves more extensive discussion and consideration than I can cover in this paper. The key message I hope I have conveyed is that I, as a leader and MHS as a company, view the management of these concepts as fundamental to our role as data stewards. As I was finishing this paper, the Canadian government announced sweeping new privacy legislation as part of a large-scale move by countries around the world to regulate and manage these issues (including GDPR, PIPEDA, HIPPA, CCPA, and others). It still comes down to decisions made by both organizations and individuals to ensure that we collectively understand the responsibilities of data stewardship and to act accordingly. Otherwise, we risk exposing potentially useful technology to bans.

One of the greatest threats to improper corporate decision-making around data stewardship comes from the fact that many organizations do not consider themselves data companies. They do not internalize their responsibilities as data processors and do not understand the individuals' data that their systems collect and store. Every corporate leader has a responsibility to be fully aware of all the data they collect on individuals and ensure that organizational policies, procedures, and responsibilities are associated with managing this data. Corporate leaders must further ensure that all employees understand that data stewardship is the responsibility of everyone in the organization. Downloading the implementation of data stewardship policies within the organization is acceptable; offloading the responsibility for creating data stewardship frameworks and policies is not. As an organizational value, this responsibility rests solely with the CEO and, if applicable, the Board of Directors.

Data is the foundation of my organization. As a CEO, I take responsibility personally for the data we manage on behalf of clients. It is my hope that all organizations are having open and transparent dialogues with their internal teams to understand the data they collect, how they create value from data, how data is stored, how they protect that data, how they use that data, and how they are processing and or monetizing that data. Only then can they understand what current and evolving legislation and regulatory frameworks apply to them and how to remain compliant. Further, I hope my peers are reflecting on how they can go beyond compliance to create frameworks that can easily be communicated to clients, build trust with internal and external stakeholders, and protect their firms from inadvertently becoming the next headline.

I haven't come across a comprehensive economic analysis that examines the worldwide repercussions of data security and privacy breaches in a general sense. However, it's safe to say that this is not an analysis any CEO or their board or directors would prefer to undergo after their organization has made headlines for such breaches. Hence, data stewardship must be a core organizational value, not just an IT department's responsibility.

Hazel

Hazel Wheldon
Chief Executive Officer
Multi-Health Systems Inc.

Have Questions? Get in touch with our team!