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 responsibility 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 behaviour, to arrive at predictions, and to develop effective interventions. As such we believe that it is imperative we have a well-articulated and easy to follow framework for trust that governs how we engage with others and how we 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 4 pillars, ethics, stewardship, transparency and accountability. This paper delves deeper into the second of the four pillars in the MHS Trust Framework, Stewardship, with a focus on Data Stewardship.

December 2020

The Miriam-Webster dictionary defines stewardship as:

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

Data stewardship then would be 'the careful and responsible management of dataentrusted to one's care' and the key to that definition is that this data is entrusted to us for use, not provided to us as our own.

As **stewards** of confidential and sensitive data, we will ensure 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 within, meeting both the intent as well as the letter of each countries data frameworks. Where national laws of origin, process, and transaction vary, we will work to the most stringent of the 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, with regards the careful and responsible management of 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 that has 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 absolutely clear, MHS does not and will not ever 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.

I would like to delve a little deeper into each of these concepts starting with data security and data privacy. These two concepts are tightly comingled and intertwined. Simply put, you can't have data privacy without data security.

Data Security

In a paper and pencil world, data security would consist of filing assessments that have been completed on paper in a secure filing cabinet with restricted access. The data is, therefore, secure and provided access is managed it is also private. Extending this base scenario to the digital realm, if the data is on a password protected laptop, an encrypted hard drive, a secure cloud server, and access is again restricted, privacy and security are maintained.

Under data security practices we also consider things like how and where data is stored, what are the policies and practices of the company I am sharing this data with and what are they doing to prevent data breaches and unauthorized access?

There are so many case studies I could cite of data breaches with new ones making headlines every day. One that stands out for me is the Equifax breach. Equifax is a company that exists to monitor your credit rating and protect you from identity theft. The fact that the personal data of over 148 million people was exposed is an epic failure.

While hackers make for great headlines, most examples of data security issues are resolved down to just plain poor decision making or lax corporate oversight. Recently, for example, Facebook made the news by exposing for years personal passwords, in clear text, in a database that was available to a wide range of Facebook employees. Someone somewhere did not pay attention to the fact that the database was unsecured. Poor human judgment and a reminder that common sense is remarkably uncommon.

Data Privacy

Data privacy is more complex. I can have the most secure data in the world, but I can still use that data in way that violates privacy. How many times have you been in a coffee shop, an airport lounge, or even on an airplane and you can see the screen, files, paperwork of the person working beside you? The data is secure in its storage but not private in its use. Equally, when data can be identified to its source, privacy can be at risk of violation.

Several recent high-profile examples of data privacy issues include a defect in Apple Face-Time 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 aren't aware that Alexa devices share audio with third parties for training purposes without permission.

Data Processing

Data processing relates to the collection, transferring, enriching activities such as scoring and reporting, and general analysis of data. Processing responsibilities were really brought to the forefront of management attention through the introduction of the GDPR legislation. If, for example, you send a wire transfer overseas, personal information (your name, 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 of the utmost importance and highlights data processing responsibilities.

Data Monetization

Data monetization is a highly charged issue. Most of us are unaware of how extensively organizations are monetizing our personal information. Few of us take the time to read the terms and conditions associated with websites, subscription services or Apps that we use – and really, who among us can read that much legal prose and have it make sense? Yet, how many times are we surprised when after searching for something on Amazon or a search engine, ads for that very same product or a related item show up the next time you open your favourite websites? Amazon, search engines, product review sites all use your search history, within their site and across affiliated sites, to create and sell targeted advertising to 3rd parties for placement on your favourite online sites. This activity is carried out in real time, by algorithms and artificial intelligences, using the best and most currently available data about your wants, ideas 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?*

Each of these data stewardship components is more complex and worthier of much greater discussion and consideration that I can devote in this paper. The important theme I hope I have conveyed is that in aggregate I as a leader and MHS as a firm consider the management of these concepts core to our role as data stewards. As I was finishing this post, the Canadian government announced sweeping new privacy legislation part of an increasingly move by countries around the world, in an attempt 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 make serious effort to understand the responsibilities of data stewardship and to act accordingly. Otherwise we risk exposing potential useful technology to complete bans such as the ban against facial recognition in San Francisco just announced.

One of the greatest threats to inappropriate corporate decision making around data stewardship comes from the fact that many organizations do not consider themselves as data companies, they do not internalize their responsibilities as data processors, and/or they do not understand the data that their systems collect and store on individuals. Every corporate leader has a responsibility to be fully aware of all the data they collect on individuals and ensure that there are organizational policies, procedures and responsibilities associated with the management of this data and to 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, that rests solely with the CEO and if applicable the Board of Directors.

Data is the foundation of my organization. I take personally my responsibility as a CEO 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 what data they collect, how they create value from data, how data is stored, how they are protecting that data, how they are using 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 my hope is that these peers of mine are reflecting on how they can then go beyond compliance to create frameworks that can easily be communicated to clients, build trust with both internal and external stakeholders and protect their firms from inadvertently being the next headline.

To date, I am unaware of any holistic economic analysis of the global impact of data security and privacy breaches in general but suffice it to say I don't think this is an analysis any CEO or their boards wants to have to go through after they have become a headline. Hence, data stewardship needs to be a core organizational value, not just an IT departments responsibility.

Hazel

Hazel Wheldon
Chief Executive Officer
Multi-Health Systems Inc.