

An Introduction To Privacy & DC DDHT Seven Rites For Data Management

By Amali De Silva-Mitchell For 2022 DC DDHT Book Health Matters, Technologies Driving Change in Healthcare, A Community of Thought

Not every jurisdiction has privacy laws. Some jurisdictions will note, that the word confidentiality is used and applied, in their laws for business. This could apply to other information as well, if the contract or agreement stipulates it. Also, in older times “mind your own business” or it’s a private matter” or under Buddhism where it noted in the ancient world to also “mind one’s own business” were upheld, when stated by others, through manners. Now there is data collection by inanimate systems, societal norms are changing and not all adhere to the United Nation’s Human Rights Charter (1948) and Treaty of many nations and currently administered as the United Nations Declaration of Human Rights, where a citizen of the world can have an expectation to a reasonable right and level of privacy for personal dignity and protection.

So why is the privacy of the person and health information discussed and prized by certain societies, when there is an imminent need for data sharing, for use, for a variety of purposes, such as development of pharma care products? It comes from the basic right that each individual has the right to a level of privacy and the ensuing data and it’s control, as noted under the UN Charter of Human Rights and more recently under data governance laws such as in Europe, the United Kingdom and Canada.

This means that a person has control of themselves, not just the physical but the information that identifies them, which provides more dimensions to them such as medical health. This is due to others who may create harms, unfairness, judgement through mis-information, mis-representation, mis-use, mis-direction, profiling, association and other ways of using information, that will remove the fairness for people as they are serviced, delivered or observed by others. This can also go into the criteria used to hire people, due to the costs of accommodation, access to health insurance, education and transport costs due to accommodation, rental of housing, wait-listing or prioritization linked to finances due to health, associated issues and so forth. It is possible that whole countries can get impacted, let alone a person or specific society due to factors of bias that may be applied to data that in the extreme could even lead to financial ratings of countries and their ability to borrow money and receive investments.

The matters of privacy stem around the data gathering (consent), the data sharing (consent), retention (safe and secure), use for which the data was collected (mis-representation), and then eventually destroyed (safe and secure) or updated (current, timely representative data). As our data gathering, storage, sharing get connected internationally, there is an imminent need for data management and sharing harmonization internationally. Also, there must be harmonization in understanding use changes to the data collected, as well as for data disposal standards.

Some companies may not want to engage with a jurisdiction that don’t have the same privacy laws as it may put them at risk in their own jurisdiction. This means that the patient will not have the widest access to the best products available. Testing may not occur in a jurisdiction for the same reason and hence people of that group living in other jurisdictions may not get the benefit of a pharma care product tested and fine-tuned for their specific ethnicity, age or gender.

It is possible for companies and others to set up clear contractual terms to over come the obstacles of data sharing amongst jurisdictions. However, this could be a cost and stumbling block for Small and Medium Size entrepreneurs seeking data to develop their systems. Not all jurisdictions will be accepting of laws that are new to their societal norms. Even if the laws are put in place the practice may be limited and the monitoring slim, hence quality and ethical data sharing could still remain an issue.

Hence, there is a real need for anonymizing patient data so that it can be shared openly for medical development use. internationally. This will also help when the medical systems are applying artificial intelligence AI and

connecting with a wider spectrum of AI interconnected systems where through reverse engineering, a data profile of a specific individual could emerge.

Statistical research processes are being developed. However, as these techniques are still new, they are not universally accepted or applied. Just as data collection is not standard, privacy application is not standard even within a defined jurisdiction. Privacy is a key value to be developed for a fair human civilization that shows respect for the person as defined under the United Nations Charter of Human Rights. As such there is a need for education and knowledge sharing on already established privacy values, principles and laws so that we can all understand and value what the benefits of privacy are and design privacy compliant innovation for data sharing internationally, for the future and for universal healthcare benefit.

The United Nations recognized Dynamic Coalition on Data Driven Health Technologies has Seven Rights or Rites (which means a question is asked about the data, and if it is of suitable quality, maturity and intent to pass to the next phase) of Passage for Data, Data Systems and Data Application as under well as for Artificial Intelligence, Quantum Applications or Statistics etc. Attention must be paid to data at 7 key points, which, if well applied and managed, will lead to successful outcomes, trust, reputation, speed of uptake and resiliency.

They are:

1. A multistakeholder approach for Context and Intent of the application and its expected outcomes (vision the international public sharing and use of data)
2. Diversity and Inclusion in all of its forms (reduce bias, increase fairness and equity)
3. Designs (including Greening & Waste), Data Management and Ethics (values and norms of different jurisdictions and harmonization to common values and norms)
4. Protections from harm, Privacy and Security (varies by jurisdiction)
5. Communications of Human and Technology and interaction there-of (HCI and what is personal?)
6. Inter-operability and Connectivity (Internationally)
7. Feedback, Risk Monitoring and Bettering (& Best Practice) for Resiliency
8. Attention to Delivery, Service, Maintenance (with ethics) & On-boarding

On the last point, as we move to 5G and 6G communications, it is currently thought that the onboarding will become easier. However, there are policies that the ehealth and mhealth device and service user must agree to, such as privacy or data use policies amongst other agreements or implied matters. This all requires a level of education or support to the end user, to enable. Not all citizens of the planet have the technical or legal knowledge and there must be compassion applied and assistance provided to all with onboarding. Care must also be taken that citizen who choose not to onboard are also taken care of in a fair manner.

References:

[Data protection in the EU | European Commission \(europa.eu\)](https://european-commission.europa.eu)

[Data protection - GOV.UK \(www.gov.uk\)](https://www.gov.uk)

[Summary of privacy laws in Canada - Office of the Privacy Commissioner of Canada](https://www.priv.gc.ca)

[Universal Declaration of Human Rights | United Nations](https://www.un.org)