HealthManagement.org
The Journal
LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES
VOLUME 19 • ISSUE 4 • 2019 • € 22
ISSN = 1377-7629

Monitor Me!

9 771377 762006 08

In Data We Trust

An efficient mHealth network relies on patient data but provision of such data requires confidence that it is being sourced and used with integrity. HealthManagement.org spoke to three health data experts for their views on what healthcare can do to secure patient trust when it comes to accessing and using their data.

Jaana Sinipuro

Project Director, Sitra, the Finnish Innovation Fund
Helsinki, Finland

jaana.sinipuro@sitra.fi

sitra.fi

@jsinipuro

The citizen's perspective and data protection issues must be taken strongly into consideration in the planning of operations and operational practices for a national one-stop shop for healthcare data. The new actor must be able to work transparently. For instance, an information security audit provides a holistic picture about the current state of data processing in an organisation and an assessment about the realisation of data protection, data security and privacy protection. It is essential that the new actor will, at the very least, conduct an information security audit of its operations and ensure the data is handled in a secure manner.

However, for a data-driven economy to succeed there are also several dimensions on trust that are critical at the enterprise level as stated in a recent survey conducted by KPMG in October 2016 on data and analytics (KPMG 2016). When an enterprise plans for its strategy on analytics, the KPMG report recommends that they build a systematic approach that spans the lifecycle of analytics and focuses on four key anchors of trust: quality, effectiveness, integrity and resilience.

These are crucial dimensions even when planning for one-stop shop for data. For winning the trust from the researchers and companies aiming to use the data, we need to ensure transparency and an audit trail to the data sources, and maintain good quality of data management tools and processes.

The same applies for enriching data sets with personal data for more tailored digital services. An international survey reveals that people's lack of trust presents an obstacle to the growth of digital business. The progress enabled by artificial intelligence is also at risk if access to data is compromised or transparency is not ensured.

John Bullivant

Chairman,
Good Governance Institute Advisory Group

john.bullivant@good-governance.org.uk

good-governance.org.uk

@GoodGovernInst

There are three types of data: personal, collective and identification. Personal data must be treated as part of the individual's body and integrity. It belongs to them and must only be taken and used with consent. It must be treated with respect and collected, used and disposed of in that spirit. Collective data is something else. We as a society need that data to understand and learn more about the human condition and how to protect and support our common good. In both cases we must be able to trust those who have access to the data. Trust is easily lost and hard to rebuild. The data will inevitably be lost, stolen and abused so those charged with its safe keeping must develop agility in responding to these failures with integrity and transparency. The third type of data is more difficult; it is that concerned with identification: fingerprints, DNA, facial recognition etc, often collected for public protection and collective security reasons but the question of trust remains. There is also a fourth: social media and the mistakes we all make in casually releasing too much information. Good Governance requires us to tackle all of these from the first principle that all data about me is mine forever and only I can determine who uses it and to what ends. We may have to compromise that principle but we must do so thoughtfully and transparently.

Marina Gafanovich

Internist, NewYork-Presbyterian
New York, USA
drgafanovich@gmail.com

mynycdoctor.com

@drgafanovich

One of the best ways healthcare can protect patient data and maintain their trust is by ensuring that access to this data is restricted to only those who require it. Information related to a patient's personal health and body is very sensitive and private. In order to ensure that this information is secure and accessible only to people who need it to provide quality patient care, the healthcare system needs to be proactive. They need to educate their staff and make them understand the meaning of privacy; they need to put measures in place that would restrict access; they need to mitigate network-related and device-related risks; they need to implement controls regarding data usage, and they need to closely monitor and conduct regular assessments. Only with a proper system in place can you secure patient trust when it comes to information that is related to them.

REFERENCES

Data and Analytics: the power of trust 2016. KPMG. Available from home.kpmg/na/en/home/insights/2016/10/data-and-analytics-the-power-of-trust.html