SECURITY EUROPE™

Security through knowledge.

Euro-View: Jacques Bus on health data security

Europe needs a far more secure "eco-system" for healthcare data

More and more data is being collected on and by patients, stored on social platforms and the cloud, and used for commercial purposes. Alongside this activity is the rising risk of data leaks or breaches. And when these happen, patients lose trust in the management of their health data.

How big is that risk? Current studies show that privacy and security are given low priority in the development of health data applications. This raises serious issues of security and safety in the field of health data. In a word, we need to drag this sector toward far higher levels of data security.

My own organisation, the Digital Enlightenment Forum (DEF) has been focused on this topic. Along with the European Commission, the Dutch Ministry of Health and Philips, we jointly organised a conference on trusted data management in healthcare in early June to explore these issues with policy makers, experts in technology and health care and industry officials.

There are three broad factors at play. First, patients are no longer passive recipients of care, and want to control their own health information. Second, the continuity of health care must not be hindered by organisational barriers between care provider "silos" that stretch across the primary, secondary and after-care sub-sectors. And third: healthcare must be seen as a "learning system" whose outcome and quality are gauged and whose feedback recycles again into care practice.

Security of data runs across all three of these area. For example, a recent UK survey found that 66 percent of 79 health data applications (apps) tested did not use data encryption – yet all of them were accredited with the UK's National Health Service! Ninety percent of the apps transmitted data to the cloud, but one-fifth of them had no privacy policy. Of those with a privacy policy, 78 percent did not adequately describe the nature of the personal information being transmitted.

Obviously, such statistics point to a serious risk of unwanted data dissemination to third party services – without a clear notification to, and consent by, the end-user.

A pan-European study on the privacy of health records known as the "PACT" (Public Perception of Security and Privacy) project found that up to 60 percent of respondents worried about different levels of access to their health data, with only 38 percent agreeing that healthcare providers offer effective data security.

Indeed, healthcare providers are rapidly moving data to the cloud, yet many of the applications they use do not incorporate appropriate security safeguards. A recent investigation by security firm Compass that trawled Google Docs and Dropbox found thousands of sensitive documents from hospitals, schools, and corporations.

Such challenges mean Europe must commit to the creation of digital and cloud-based ecosystems for personal health data management. These should be based on realistic cost assessments and international standards for content and platforms, while minimising the distribution of health data beyond health professionals. At the same time, existing European regulation should be strengthened and enforced such as the EU's General Data Protection Regulation or the EU's Network and Information Security Directive in order to create a more robust legal framework.

Empowerment of citizens through smart regulation, including the legal right to a digital copy of all personal data, should be the overall goal, leading to an innovation-friendly ecosystem for healthcare data.

Yet the sector has been slow to reap the benefits of the digital revolution. Technologies such as the "internet of things" (IoT) and big data offer many opportunities for health service providers and individuals. But users don't yet expect the same standards of service, conven-

ience, security and trust in healthcare as we do from other sectors such as banking.

For example, Switzerland's citizen-owned, non-profit "MIDATA.coop" is based on the banking model. It is based on the assumption that each participating individual has a constitutional right to a digital copy of all their personal data, whether medical or non-medical. This is deposited in a safe and secure 'data bank account' for managing and sharing data on transparent terms.

The MIDATA.coop rests on open source code and operates with the highest security standards, based on data encryption. Revenues from any approved secondary use of the data will be invested in projects and services that benefit its members and society at large. Its ultimate goal is a federation of national personal data cooperatives based on a common IT structure and data exchange platform, similar to the way SWIFT operates for its financial exchange members. We think this innovative approach should be taken up in all Member States.

The United States has also achieved notable success with regulations that set the standard for protecting sensitive patient data. In recent years these laws have been extended to cover cloud services – and they are strictly enforced. As a result, any company in the US that deals with protected health information must ensure high levels of transparency.

Although the health economy and regulatory environment in the US are very different from those in Europe, we think our region could profit well from the healthcare data protection experience of other countries.

Jacques Bus is secretary general of the Digital Enlightenment Forum (www.digitalenlightenment.org) and can be reached at jb@digitrust.eu.

SE

Published by:

SECEUR™

Brooks TIGNER, Chief Policy Analyst & Head of Technical Studies

Teri SCHULTZ, Policy Analyst

Chris DALBY, Policy Analyst

Robert DRAPER, Business Development Director