FORBRUGERRÅDET

May 2010

Health IT Systems Must Address the Needs of the Consumers

Consumers of health IT systems are broken up into two groups –
healthcare patients, whose treatment and private data are affected by systems; and healthcare providers

Issues Faced by Patients...

- **Danes are not worried about their medical data**
- **Doctors can access any patient's data through health IT systems**
- **Widespread use of the CPR number is dangerous**
- **Large, centralized systems for healthcare make the CPR even more dangerous**
- **Technology for patients is difficult to use**

Danes are not worried about their medical data
Most Danes are unaware about where their data are stored, how their data are accessed, and what they can do to keep their data safe. Even if abuse of private data is not yet a major problem, there is no guarantee this will be the case in the future.

Doctors can access any patient's data through systems
Right now, using EHR systems, any doctor can access any patient's data, regardless of their relationship to the patient, even if it is illegal to do so. Doctors' access to patient data is logged, but only 1-10% of the logs are actually reviewed. This system does not protect patient privacy – even if a doctor is caught, the damage is done.

Widespread use of the CPR number is dangerous
The CPR number is used to access many important systems. If an attacker breaks into any of these systems and finds a citizen's CPR, they can use this to break into all of the other systems that use it. The coming **NemID** system, while more secure, suffers from the same problem – if a citizen's NemID is compromised, all of their data can potentially be stolen.

Large, centralized systems for healthcare make the CPR even more dangerous
The trend of using very large health IT systems that contain lots of data adds to the risks of the CPR number. Attackers have even fewer systems to break into. System administrators also have total control over patients' sensitive data, and can view it without anyone's knowledge.

Technology for patients is difficult to use
Technology associated with EHR is difficult for patients of certain demographical groups. Patients may have a difficult time using a computer to properly to access their medical information or remembering all the passwords needed.

Issues Faced by Healthcare Providers...

Large systems are too difficult to customize
The large, universal systems that are commonly used as health IT solutions are too difficult to customize when addressing healthcare providers' specific needs. Different fields of health care each require specialized system for the technology to be most effective. Large systems also take much longer to upgrade, since the entire system must be upgraded all at once by the vendor.

Data standards are not strict enough when implemented in health IT systems
Standards for healthcare data that allow two different health IT systems to communicate are ineffective. When vendors decide to use current Danish standards, the implementations can be different enough such that two systems using the same standard cannot share data. Larger companies that sell systems can overlook standards and create systems that are not easily interoperable with other vendors' systems. Thus, when a hospital buys a system from that company, they are "locked-in" to that system, because any new systems they buy will not work with the old system.

Additions and stipulations to laws cause too much confusion
Danish laws on electronic data accessibility have become more complicated and too confusing for providers. In some instances, this causes providers to care less about privacy and security issues. In other instances, providers are wary and refuse to access potentially critical data because the provider is unsure of the legal repercussions.

Data accessibility laws contradict treatment requirement laws
Healthcare providers other than doctors, such as nurses, cannot access patient records even though they need this information in order to properly treat a patient. The law must allow nurses and other groups to access the data they need to properly perform their duties.

- **Large systems are too inflexible for providers' needs**
- **Data standards are not strict enough when implemented in systems**
- **Additions and stipulations to laws cause too much confusion**
- **Data accessibility laws contradict treatment requirement laws**

The Danish Consumer Council is an independent consumer organization which represents the consumers' interests vis-à-vis business and authorities. We are an umbrella organization covering 27 national organizations and five local consumer groups.
Visit our website on www.fbr.dk, and subscribe to our daily newsletter: www.fbr.dk/nyhedsmail/.
The Danish Consumer Council publishes the leading consumer magazine in Denmark, Tænk: www.taenk.dk.
Side 1 of 2

Forbrugerrådet (Danish Consumer Council) Recommends...

Spread awareness about patient privacy issues

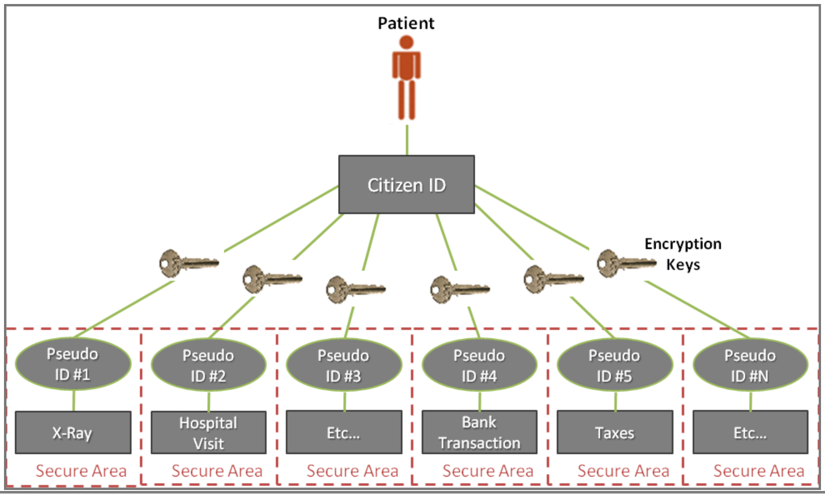
Patients must be made more **aware of the significant risks to their privacy** so that they can take the proper precautions. Public awareness of privacy issues will also motivate both the industry and government organizations to focus more on keeping patient data private.

Use role-based access control to prevent illegal access of data

Role-based access control in systems **allows healthcare providers to only access the data of the patients they are currently involved in treating.** This will help prevent providers from illegally accessing data. Providers will also no longer have to interpret potentially confusing laws to decide whether or not they can legally access a patient's data.

Use pseudonym systems for patient identification

Pseudonyms can be used to identify users in IT systems in place of the CPR number or the NemID system, without using personal identifiers. This will **vastly reduce the significant privacy risks to citizens** caused by the Danish CPR number. The figure on the right depicts a pseudonym system — patients use a different ID instead of the CPR for every system so that an attacker must break into each one individually. Pseudonyms will allow patients to keep control of their data. Pseudonyms also naturally support the use of small modular systems and discourage the use of large, centralized systems.



Create stricter data standards with less room for different implementations

Using stricter interpretation of standards would **promote interoperability between systems and empower smaller vendors of health IT systems**, creating more competition in the market. Stricter standards would also make small modular systems more feasible.

Aid vendors in adhering to data standards

An organization that helps vendors properly adhere to data standards would reduce differing implementations and encourage vendors to ensure that their systems are interoperable with other systems. This would be much more useful than current organizations, which only check to see if vendors are properly following standards and do not offer any help.

Clarify contradicting laws relevant to health IT

A revision of the laws related to health IT issues to remove contradictions would reduce complicated situations in which a healthcare provider must decide which law to follow at what times. **A compilation of laws and regulations of privacy and interoperability pertaining to health IT into one document** will help healthcare providers to quickly look over relevant legal information if necessary.

Implement smaller, modular systems instead of large systems

Using smaller, more modular health IT systems instead of larger, universal systems will be **more flexible to fit both healthcare practitioners' and hospital administrators' needs.** Upgrades to specific parts of systems can happen more rapidly as well. This is very important for security technology, which must be as modern as possible in order to be effective. Using smaller systems will also help prevent "lock-ins" to large systems.

Design systems with both patients and providers in mind

If vendors work directly with users when creating systems intended for both patients and providers, it will ensure that new systems are of the highest quality and that their **systems are practical and effective for their users**. Using modular systems will also give providers wider choice in selecting the most effective system for their needs. **Vendors must also conduct Privacy Impact Assessments (PIA)** when creating systems, which involves finding all potential privacy risks and creating the necessary counter-measurements.

The Danish Consumer Council is an independent consumer organization which represents the consumers' interests vis-à-vis business and authorities. We are an umbrella organization covering 27 national organizations and five local consumer groups.
Visit our website on www.fbr.dk, and subscribe to our daily newsletter: www.fbr.dk/nyhedsmail/.
The Danish Consumer Council publishes the leading consumer magazine in Denmark, Tænk: www.taenk.dk.