THE Open GROUP

How to Put Open FAIR™ Risk Analysis Into Action

A Cost-Benefit Analysis of Connecting Home Dialysis Machines Online to Hospitals in Norway

A White Paper by:

Mike Jerbic, Sushmitha Kasturi, and Biljana Strageland, PhD

May 2017

How to Put Open FAIR™ Risk Analysis Into Action

Document No.: W176

Published by The Open Group, May 2017.

Any comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by email to:

ogpubs@opengroup.org

Table of Contents

Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

This White Paper provides insight into the benefits and costs of connecting home dialysis machines online to hospitals, and the security and privacy risks of such connections.

It offers an Open FAIR analysis of security and privacy risks, comparing those risks to the likely benefits of connecting home dialysis machines online to hospitals, and concluding that while the prohibition doesn't likely make much difference today, it could going forward, if policy-makers ask the right questions.

Introduction

The Kingdom of Norway is a constitutional monarchy and parliamentary democracy of approximately 5.2 million people. With GDP *per capita* of about $75,000 USD, it ranks ahead of most developed Western economies, including the United States GDP *per capita* of about $56,000 USD. In Norway, about 11% of its population suffers from chronic kidney disease, and in 2012 about 1,240 people suffering from end-stage renal disease were on sustained kidney dialysis. That number is growing at about 5% per year.

Dialysis treatment is expensive. Each newly diagnosed patient who requires dialysis represents a net present value in treatment cost between $148,000 to $316,000 USD, and this cost does not include the costs to the patient such as time lost in treatment, travel time to and from treatment centers, and other quality of life implications associated with treating chronic end-stage renal disease this way. As agents of Norway's people, four Regional Health Authorities (RHAs) are responsible for treating these patients cost effectively. Inside the RHAs, doctors, hospital administrators, and Enterprise Architects all are trying to offer alternative treatment methods that improve patient quality of life outcomes while reducing total social costs.

High treatment costs coupled with a growing patient population present an opportunity for innovation, and some companies are providing home dialysis treatment options that cost the RHAs less than equivalent treatment onsite. Security and privacy policy set by RHA security and compliance people, however, limit the convenience of these innovations. Specifically, the information security architects and compliance people prohibit online connection of home dialysis machines because of perceived security and privacy risk, yet Enterprise Architects see significant patient value in relaxing that prohibition. Architects challenge the security and privacy policy enforcers to allow online connections between home dialysis machines and hospitals to improve patient convenience and quality of life. They essentially want an answer to the question: What are the benefits and costs of preventing home dialysis machines from connecting online to hospitals? Do the security and privacy risks of these online connections outweigh the benefits to the public and patients?

This White Paper provides insight into that question, offering an Open FAIR analysis of security and privacy risk, comparing those risks to the likely benefits of connecting home dialysis machines online to hospitals, and concluding that while the prohibition doesn't likely make much difference today, it could going forward, if policy-makers ask the right questions.

The Problem the Research Team was Asked to Investigate

Home dialysis requires that patients exchange treatment data with their physicians. Under the current policy that prevents online connections between machines and medical services providers, the exchange is manual. Patients must physically transport their data on an external device, such as a USB thumb drive, to the doctor. The doctor reviews that data and, finally, the doctor may update dialysis parameters, some of which are communicated to the machine via the physical medium. This process is time-consuming to the patient and costly to the RHAs. Patients value the time spent in transportation, and the RHAs reimburse patients for travel costs, including the cost of a taxi to and from the medical facility. Architects assume that patients must make these trips after each dialysis session: three times per week for each of 52 weeks per year.

In the scenario that follows, an Enterprise Architect suggests that, to save patient and public resources, the security and compliance people who manage internal hospital IT systems allow direct connections between the home dialysis machines and the hospital data systems. Doing that would automate the data exchange and

preclude up to 156 patient trips to the facility, both improving patient quality of life and reducing costs of travel.

Norway's medical service providers are not allowed to connect any information system with sensitive patient data to the Internet. Internal hospital information technology policy prohibits these connections on patient privacy and hospital information security grounds. If an architect proposes to open a connection, a typical dialog between that architect and the service provider's compliance and security team might look like this.[1]

Architect: My question to security was: Why can't we read and update treatment data and plans online? This would give us the following benefits:

1. It increases life quality for the patients because they don't have to spend time travelling to the hospital, spend hours two to three times waiting for the stick, and then go home again. The data will be available 24/7 for monitoring at the hospital, which increases patient security, and you can have continuous adjustment of treatment plans. The patient can live a much more uninterrupted life.
2. The doctors don't have to wait in the office for patients who may or may not show up according to scheduled visits, and then reschedule no-shows. The data is available whenever the doctor is and gives much better time management for the clinicians who then can spend time treating patients instead of waiting. This frees up resources, time, and money at the hospital.
3. More "demanding" patients can be offered home dialysis treatment because you can have close monitoring online during the treatment process, which again frees up resources, time, and money at the hospital.
4. And so on …

The ensuing conversation with information security (Security) and the architect (Architect) goes something like this:

Security: No, the network transport is not secure.

Architect: And a memory stick is? Besides we already have a VPN solution in place. We can use that.

Security: No, the VPN solution cannot be used to connect to patient-sensitive solutions.

Architect: Okay, then let's put crypto equipment in both ends and secure it that way.

Security: No, we don't have a policy for that, besides we don't have control over the end computer at the patient's home.

Architect: Then let's give the patient a secure computer we can control.

Security: No, we don't have a policy for that.

Architect: (unintelligible …)

[1] From an email conversation between Stig Hagestande, Enterprise Architect at Sykehuspartner HF, Shared ICT Service Provider for the South East Regional Health Authority in Norway and Mike Jerbic July 27, 2016.

Further conversation showed that fear, uncertainty, and doubt about risks associated with privacy, malware introduction, and ransomware were the dominant causes of this conversation. Security teams fear that the connected home dialysis device could inject malware or ransomware to the medical service provider's systems, and that possibility was an unacceptable risk to take. Similarly, exposing a patient's data to any possible interception online was unacceptable. Absent any case-specific analysis, the fear, uncertainty, and doubt over the mere possibility of losses from connecting home dialysis machines online to medical services providers alone are enough for policy compliance and information security architects to impede or veto proposals that if adopted would improve both the healthcare system's efficiency and patient quality of life outcomes while reducing taxpayer costs.

The scope of the analysis included analyzing and estimating the risk associated with connecting the home dialysis machines online to the medical services center IT network, estimating the benefits foregone, or opportunity cost, of maintaining the *status quo*, and comparing the two. As a result of this analysis, the team believes that although prohibiting the proposed online connections between dialysis machines and service providers is not a material cost or benefit today, a bigger question lies in the social policy surrounding online telemedicine. If the experience of other regions is representative of what would likely happen in Norway, connecting a broader array of information and communication technology online to hospitals likely improves patient outcomes and reduces costs. More research is needed to determine important correlations between online connectivity and cost-effective treatment modalities.

Analysis of the Security and Privacy Risk: An Open FAIR Approach

Prohibiting the connection of home dialysis machines to hospitals, treatment centers, and physicians has an opportunity cost felt by patients, hospitals, and taxpayers. Patients lose convenience, quality of life, and, some research shows, improved healthcare outcomes. The question is, how do these forgone opportunities compare with the benefits that the prohibition contributes to safety and security? What is the risk avoided by prohibiting home dialysis machine data communication to hospitals, treatment centers, and physicians? Do the benefits of avoiding these risks exceed the opportunity costs of mitigating or accepting them?

To answer this question, the team analyzed three risks associated with data connectivity between home dialysis machines and hospitals, risks that hospital regulatory compliance and information security architects put forward as their reasons to resist hospital to machine connections via the Internet. These risks (the probable frequency and magnitude of future loss) were articulated as:

- The risk associated with malware introduced by the Healthcare Data Management (HDM) and transferred to the hospital via remote data connection
- The risk associated with ransomware introduced by the HDM and transferred to the hospital via remote data connection
- The risk associated with loss of patient privacy from unauthorized disclosure of private medical treatment information while exchanged by the HDM and the hospital through the remote data connection

Using the Open FAIR methodology as the model to estimate these risks, the team concluded that all of them can be made as arbitrarily small as desired, that these risks depend upon the architecture of implementation, and that technology exists to reduce them to any level desired. The substantive question this analysis discovered is not: "Do the benefits of avoiding these risks exceed their opportunity costs?", but: "Can IT architecture, engineering, and implementation teams design, develop, and implement a cost-effective technical solution to manage these risks to the point that the probable losses of accepting the residual risk are less than the benefits received from accepting it?".

Case-Specific Analysis: Reducing the Uncertainty and Doubt, if not the Fear

The security and compliance teams feared two sources of risk: the risk to the hospital associated with malware and ransomware and the risk to the patient associated with the loss of control over the privacy of his medical record information. These two risks must be analyzed separately then aggregated to determine the total risk decision-makers were concerned about. In both analyses, Open FAIR was the risk analysis method used to decompose each risk into its loss scenario and risk factors, conceptually discuss those risk factors, and estimate the likely severity of the probable loss frequency and probable loss magnitude. This section highlights those two analyses.

The Risk Associated with Malware and Ransomware

The stylized scenario consists of an online connected dialysis machine transmitting malware or ransomware to the hospital's information network. In this analysis, the hospital or healthcare system is the primary stakeholder, which now is just called "the hospital", that has an information asset exposed to some loss. To scope this analysis, the team had to identify who wanted to impair the asset, the threat agent, and how that

threat agent impaired the asset to cause a loss, the threat vector or means through which the asset was compromised.

The primary stakeholder was easily defined or determined to be the medical services provider, whether an RHA, a hospital, a physician's office, or other facility that directly interacted with the patient in delivering dialysis treatment and care.

The threat agent, too, was easily defined or assumed to be an agent external to the hospital who had a financial incentive to compromise the hospital's data system. Any threat agent internal to the hospital would likely achieve a data manipulation or theft objective more easily than penetrating a home dialysis machine. After all, threat agents too are assumed to be rational, economic actors who want to achieve their objectives at lowest total cost. There likely is an easier way to get what that agent wants on the inside of the hospital than outside.

We also assumed threat agents were financially motivated. Penetrating a small number of specialized home dialysis machines didn't seem compatible with the motives of non-financially motivated threat agents such as curiosity seekers, data vandals, social "hacktivists", state-sponsored terrorists, or other threat communities. Especially in the case of ransomware, the financial motive appeared to be the only one worth considering.

Determining a reasonable or likely threat vector, however, was problematic because it depended upon the information systems architecture between the hospital and the home dialysis machine. In researching architectural approaches, we believed that common, off-the-shelf technology and methods are available to reduce the likely frequency of threat events to an arbitrarily small level. In other words, using common technical controls such as intermediary drop boxes, data validation and verification before data use, and digital signatures would make an online connected dialysis machine highly resistant to a threat agent's injecting malware or ransomware into the hospital and to the hospital's using tampered data unknowingly. As the results of any risk analysis depended directly upon the online system's architecture, which was not specified in advance, the analysis essentially stopped, but it did reach this conclusion:

The risk associated with malware and ransomware depends upon the architecture of the dialysis machine, its interconnection with the hospital, and the hospital's use of transmitted data. Without specifying that architecture in advance as context, the analyst cannot reasonably estimate the risk, but can recognize that available technology can arbitrarily reduce the risk to any desired level approaching zero. The risk question can be reframed into an architectural and engineering challenge. The question to be answered is not one of what is the risk, but how to architect, design, implement, and maintain a system that meets management's acceptable level of risk at an acceptable cost. If this challenge can be met, then the benefits of accepting the residual risk outweigh the cost of the risk itself.

The Risk Associated with Patient Privacy

There is a global consensus that patients should be able to control who accesses their medical records, and though privacy regimes around the world differ somewhat, they basically all affirm that unauthorized, uncontrolled access to medical personally identifiable health records is prohibited. Complying with this public policy is a reasonable objective for information security and compliance people.

Maintaining patient privacy, however, is not absolute. Instead, as in other sectors of the information economy, preserving privacy comes at a cost that is balanced by its benefits. For example, for the benefits received by online access to financial services, the public willingly accepts some risk to privacy invasion

over its financial records. Similarly, patients around the world accept some risk to their privacy for the benefits of having online access to their medical information. The question is not whether to prohibit all online access to personal medical information, but rather what is the risk to their privacy patients are willing to accept for the benefits they receive from online access.

To analyze the risk associated with privacy loss from connecting home dialysis machines online, the research team conducted an Open FAIR analysis on that risk. In scoping that analysis, the team determined:

- The primary stakeholder in this analysis is the dialysis patient who wants to use home dialysis, consciously willing to accept some risk of privacy loss for the convenience and other benefits received from that treatment mode
- The asset at risk is control over the stakeholder's dialysis information exchanged between the home machine and the hospital or physician; specifically, the privacy risk to information is the control over who can read that information and tie that information to a specific, personally identifiable patient
- The threat agent, however, was not as readily identified

  Rational threat agents need a motive to expend their limited resources to attack and compromise an information asset. In this analysis, the pay-off to the threat agent appeared speculative, leading the analysts to wonder how that agent benefitted from capturing dialysis treatment information. The team understood that dialysis machine treatment data consisted primarily of technical information related to the treatment session and could not see how a rational threat agent would benefit from capturing it.

Without a pay-off to the threat agent, why would this data become a target of the threat agent? Who wants this information? Why? Until these questions are answered, while an attack on a patient's privacy is possible, it is not probable.

Risk Analysis Conclusion

Neither losses from malware/ransomware nor privacy breaches appear probable. Is it possible threat agents want to attack hospital infrastructure through the vector of an online connected home dialysis machine? Yes, it's possible. Is it probable? This team concludes "No".

Similarly, for the risk associated with privacy loss, this team concludes that there are few threat agents who would significantly benefit from attacking patient privacy through the considered threat vector. Although a privacy breach is possible, it, too, is not probable.

Foregone Benefits – Quantifying what the Public and Patients are Losing through Current Policy

The implications between social policy alternatives can either be overt, easy to evaluate and measure, or hidden and hard to easily observe and estimate. Easy to evaluate implications include direct cost savings between treatment methods such as the savings between home dialysis compared to in-hospital dialysis. Hidden costs include the economic value of patient time lost in transit to treatment centers or quality of life outcomes that differ between treatment methods. Both must be considered to accurately estimate the forgone benefits, or opportunity costs, of social policy alternatives.

With the number of kidney dialysis patients in Norway doubling in the last decade, it is important to find cost-effective dialysis methods. Some of the modalities of kidney dialysis are hemodialysis (hospital), self-care hemodialysis (hospital), hemodialysis (satellite units like a nursing home or local medical center), hemodialysis (home), and peritoneal dialysis (home). For dialysis treatments in hospitals, patients will have to travel three times a week and undergo a six or seven hour-long treatment, all resulting in high travel costs and lost leisure time to the patient.

However, the same dialysis when done at home (home dialysis) saves about 434,000 NOK per patient per year (about $50,000 to $52,000 USD) in direct cost savings to the healthcare system. From health and societal perspectives, home dialysis is at least as or more effective and at the same time less expensive compared to other modalities. Home dialysis is often done five times a week, which usually makes the patient healthier than the three times per week in-center options. Home dialysis has comparatively better quality of life than hospital dialysis in terms of better sleep, a more active life, reduced depression, and a lower risk of cardiovascular disease, all common complications of kidney disease and dialysis treatment. As home dialysis offers improved patient outcomes at lower cost to the healthcare system, home dialysis, for those patients that are good candidates for it, represents a superior option to alternative methods. To capitalize on this option, Norway's Minister of Health has set a goal of approximately doubling home dialysis treatment in Norway from 15% to 30% by 2017 (Gustad 2017).

For this analysis, the researchers investigated the primary, narrow question at issue: What are the costs and benefits of the current privacy and security policy that prevents home dialysis machines from connecting online to hospitals or physicians? The forgone benefits of this policy compared to online connected home dialysis machines centered on direct costs avoided to the healthcare system and indirect costs to patients of foregone improvements in quality of life through increased leisure time available from avoided travel to and from the treatment center. All of these analyses were completed under the assumptions in the stylized dialog:

- Patients must move their data manually on external storage devices, such as USB memory drives, between the home dialysis machine and the onsite physician
- Patients then wait for the physician to evaluate the data and make treatment recommendations, and return home
- Patients make this journey three times per week throughout the entire year

Direct Costs Borne by the Healthcare System

Norway's healthcare system could save the directly reimbursed travel costs for patients who are moving data back and forth between their homes and the hospital/physician's office. Estimated total travel costs that could be avoided are about 227,000 NOK per year per patient, or about $27,000 USD per patient per year. In 2012, about 203 patients used home dialysis, and Norway is estimated to have spent about $5.4 million USD in direct travel costs to reimburse home dialysis patients in taking their data to and from their physicians.

Saving these travel costs is one of the largest benefits of allowing home dialysis machines to connect online with the physician. Table 1 summarizes the costs incurred from traveling to the hospital. The patients who are on home dialysis are assumed to travel with their data after each home dialysis session (about three times per week was assumed).

Table 1: Direct Travel Cost Estimates

	Average Distance per Trip (km)	**No. of Trips per Year**	**Total Travel Cost**
Estimated Home Dialysis	45	156	$27,215 USD (227,310 NOK)

Hidden Costs Borne by Patients

In the scenario, after each dialysis session patients must travel with their data to their physicians, wait for the physician to review the data, and then return home with the data and a possibly revised treatment plan. Connecting the dialysis machine online to the hospital/physician would automate this data exchange and treatment plan update, saving the patient the travel and wait time, ostensibly three times per week. How much is that time worth?

The Norwegian government values the social cost of time at the average working wage in Norway. Patients who travel are estimated to spend 4 to 8 hours per day traveling and waiting for their analysis after each home dialysis session. Some patients are not able to travel by themselves and will have a companion, so some fraction of all the patients, estimated at between 10 and 50%, have another person committing the same amount of time (and opportunity cost of that time) to support them. Table 2 shows that the total lost value of patient and companion time spent to comply with the privacy and security policy is about $37,000 USD per year.

Table 2: Opportunity Costs of Leisure to Patient and Companion (Pike et al. 2013)

	No. of Hours	**Frequency**	**Additional Variables**	**Total**
Leisure Cost (Patient)	4 to 8	3x/week => 156x/year	$29 USD (245 NOK)/hour	**$18,096 to $36,192 USD** (151,146 to 302,293 NOK) **$27,417 USD** 229,000 NOK
Leisure Cost (Companion) 10% to 50% of Patient Cost	4 to 8	3x/week => 156x/year	$29 USD (245 NOK)/hour	**$1,810 to $18,096 USD** (15,115 to 151,146 NOK) **Average: $9,953 USD**

	No. of Hours	Frequency	Additional Variables	Total
Total Annual Lost Leisure (Average)				**$37,370 USD** (343,930 NOK)

Discussion and Cost-Benefit Analysis

The above benefits were calculated based on the scenario, assumptions, and risk questions presented to us. According to all those, home dialysis patients are assumed to travel about 156 times each year to the hospital. However, further research showed that estimate was inaccurate and that home dialysis patients actually visit their physicians about 15 times per year, not the assumed 156 times, and those patients would make these trips anyway as routine health checkups, even if the dialysis machines were connected online to their physicians, automating treatment data exchange. The avoided travel cost benefits were overstated, and the privacy and security controls in place now actually have minimal opportunity costs.

Both the opportunity costs and risks are very low. We conclude that the current policy of preventing online connections is cost-benefit-neutral with the problem as described.

However, research shows home dialysis as compared to hospital dialysis has many benefits beyond saving travel costs and patients' travel time. Quality-Adjusted Life Years (QALY)[2] and quality of life[3] for home dialysis patients are both higher compared to hospital dialysis. Patients who dialyze at home sleep through treatment and have more time during waking hours to do their daily activities. Of the few studies done, most concluded that home dialysis is associated with both lower costs and higher quality of life, including improved physiological and mental parameters as compared to hospital dialysis. Improved patient acceptance of home dialysis has the potential both to improve patient outcomes and to reduce healthcare system costs, but more research is needed to quantitatively estimate the value of patient outcome improvements and the reasons why patients refuse home dialysis.

More eligible patients refuse home dialysis than accept it in Norway. If the 250 to 300 dialysis patients who are eligible for home dialysis accepted that treatment, total home dialysis across Norway would increase from 15% to 30%, saving an estimated $13 million USD (108,930,882 NOK) to $15 million USD (125,689,480 NOK) per year. The Norwegian Minister of Health, Bent Høye, wants to expand implementation of home dialysis to a larger scale and confidently envisions that "at least 30% of dialysis patients will get home dialysis" as a part of 2017 goals towards better quality and patient safety.[4] To achieve this goal, however, patients need to feel more comfortable with the technology.

Some research indicates that patients are not accepting home dialysis because they are afraid of a mishap or problem that they cannot respond to during a treatment session. It appears that emerging telemedicine technologies give patients the comfort, convenience, and security of interacting with their physicians through a secure video call system. Improved connectivity between patient and hospital/physician can alleviate patient apprehension, leading to improved adoption of the home treatment. The correlation between home dialysis and telemedicine is likely significant and, too, worthy of future research. While telemedicine has been growing in New Zealand, the UK, and Australia, Norway would need to change its policy to implement

[2] QALY is a generic measure of quality and quantity of life when a person is burdened with any disease.

[3] Quality of Life and Willingness To Pay (WTP) can be synonymously used with Incremental Cost-Effectiveness Ratio (ICER).

[4] Sykehustalen 2017: www.regjeringen.no/no/aktuelt/dep/hod/nett-tv/nett-tv-sykehustalen-2017/id2524050.

it. Critically evaluating the costs and risks of telemedicine through an Open FAIR analysis appears to be an area for further research.

Without a defined threat agent and motive, the team concluded that the risk to patient privacy was purely speculative: possible, yes, but not probable. However, in investigating this question, a different question needed to be asked. Instead of asking whether fear over a possible privacy breach was sufficient to deny online connectivity between the home dialysis machine and the hospital, is a better question one of *who* should decide? Should public policy-makers, security and compliance people, or patients themselves decide whether to accept the risk of a privacy loss for the benefits received from taking that risk? The question then becomes one not of *what outcome* (connect the machine to the hospital or not) is chosen, but of *who chooses* (patients, public policy-makers, or security and compliance people)?

To answer that question, University of Oslo law professor Marit Halvorsen said:

"In my opinion, patients must be able to choose to exchange access to their medical information. The main rule according to Norwegian law is – and must be – that medical information is confidential, as long as the patient does not agree to share it. Exceptions must be made by law and only for very strong reasons (for example, when the patient is underage or not sui compos and his/her next of kin needs the information to take proper care of the patient, or if relevant health authorities need the information for important public health purposes). Before making the decision to share their health information, patients must of course receive relevant information about possible benefits and risks.

Patients who prefer home dialysis are perfectly capable of judging the risk pertaining to the transfer of their dialysis data to the hospital via electronic devices."

From this opinion, it is unclear why information security and compliance departments should have the dominant voice in determining whether to prohibit patients from accepting this risk to their privacy.

Conclusion and Areas for Further Research

The team concluded that the immediate effect of preventing online connections between home dialysis machines and hospitals/physicians is negligible, but the research and associated risk analysis discovered that the original question at issue is not likely the "right" or a "valuable" question to ask. Better questions for further research would include:

- What is the relationship between telemedicine and the patient's acceptance of home dialysis as a treatment plan?
- What are the total social benefits to Norway from broader telemedicine adoption?
- What are the social costs, in terms of information and privacy risk, to Norway from broader adoption of telemedicine?
- Who should be empowered to make decisions on whether to accept privacy risk associated with online medical information exchange? Patients, public policy-makers, security architects and compliance people, or others?

Other regions around the world are adopting new telemedicine technologies and appear to be reducing costs, improving patient outcomes and managing information security and privacy risks associated with online connectivity between home and hospital. Telemedicine is an increasingly prevalent technology. Countries such as New Zealand and the UK that have experience in delivering online solutions to patients with end-stage renal disease have observed the benefits and the risks associated with home dialysis. As far as we can tell, the risks associated with privacy loss and information security have been manageable in each case. Home dialysis treatment has increased consistently over many years. If the security and privacy risks outweighed the benefits, we would expect the respective healthcare systems to have stopped delivering telemedicine services. That they haven't is an indicator that the risks are likely manageable, but more research is needed.

Security and privacy risk management is not the only problem, nor likely the significant problem, that impedes advanced cost-effective care delivery. To voluntarily accept home dialysis options, patients must feel comfortable with the safety of those treatments. Good, real-time remote access lets hospitals monitor and if necessary intervene in treatment and gives patients more confidence in the new technology.

For example, a 66-year old home dialysis patient Tim Evans from Southend, UK, where remote monitoring has been up and running for a few years, believes the inclusion of the remote monitoring system has helped improve his lifestyle, as he explains: *"The hospital can read my stats every day, and if they want to change something on my regime they can do so over the airwaves. This is better for me because it means that they can take care of me quickly and more easily, and it's better for them as well."*[5]

And, yes, more research is needed!

[5] See www.baxterhealthcare.co.uk/news-media/newsroom/uk-featured-stories/tim-monitoring-support-treatment-home.page?.

References

- Ellen-Marie Pedersen-Gustad: Holding his Hospital Speech Tuesday, Tidens Krav (2017)
- Eva Pike, Vida Hamidi, Tove Ringerike, Arna Desser, Ingrid Harboe, Marianne Klemp: Health Technology Assessment of the Different Dialysis Modalities in Norway, Norwegian Knowledge Centre for the Health Services, 19 (2013): 3-105

About the Authors

Mike Jerbic

Mike Jerbic is a lecturer at San Jose State University and teaches economics there. Mike led the project in this report and developed the risk analysis.

Sushmitha Kasturi

Sushmitha Kasturi graduated with her BS in Economics in December 2016 from San Jose State University and did much of the research on the opportunity costs of current Norwegian security and privacy controls.

Biljana Strageland, PhD

Biljana Stangeland, PhD has a background as a scientist in medical research. She is currently working as a Managing Solution Architect and data scientist in Capgemini Norway. Biljana gathered the information on the status of home dialysis in Norway and several other countries and helped with some medical information.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 500 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.