Journal of Biomedical Informatics 63 (2016) 226–234

Contents lists available at ScienceDirect

Journal of Biomedical Informatics

journal homepage: www.elsevier.com/locate/yjbin

Commentary

Confronting systemic challenges in interoperable medical device safety, security & usability

Elizabeth Averill Samaras (DNP, CPE, HEM)*, George Michael Samaras (Ph.D., D.Sc., PE, CPE, CQE, CBA)

Samaras and Associates, Inc., United States[1]

1. Introduction

Safety and security are negative goals. Safety, security and usability (SSU) are system properties. They cannot be isolated to a component or some layer of the system. All three are prerequisites for system effectiveness. Ensuring SSU of an integrated system requires a holistic view; a myopic view will mislead.

Consider the following illustration of a cybersecurity breach among high profile industry players [1]. Three well-respected and well-trusted global industrial leaders (Google, Apple, and Amazon) made products involved in the 2013 hacking, theft, and destruction of an individual's "digital life" – purportedly for no obvious economic or criminal reason. The victim, Mat Honan, briefly described the incident and summarized the source of the breach, as follows:

> *In the space of one hour... my Google account was taken over, then deleted. Next my Twitter account was compromised... my Apple ID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.*
>
> *...Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information — a partial credit card number — that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws... and points to a looming nightmare as we enter the era of cloud computing and connected devices.* [1, page not specified]

The hackers continued to wreak havoc by posting ruinous hate-speech to Honan's Twitter followers, and other actions that undermined his reputation. And while the author admits to his own failure to use better security safeguards, that realization is no comfort to him for losing the only copies of pictures he had of his child's first year of life because the hackers wiped his MacBook clean.

Why should anyone concerned with medical device interoperability SSU take heed of this story, other than as a uniquely modern cautionary tale? Because further examination reveals significant dimensions of the story that relate to interoperability. Each partial piece of information was reasonably safe on its own; separate examination, even today, of each of these three individual corporate entities demonstrates that their policies and procedures were reasonable and acceptable given "good practices" at that time. Pairwise examination of each of the three entities (Google-Apple, Google-Amazon, and Apple-Amazon) yields the same result; there seemed to be no obvious hazards to users. It is only when the larger system is examined simultaneously that hazards begin to be exposed. Why? Because in this case, the source of the problem was not each individual "device", nor pairs. The system that failed was comprised at a minimum of the three firms, the intended user, the malicious users with their "unintended use" of the information, and each firm's customer service employees following (or failing to follow) their internal approved procedures. The mere fact that the firms' products were not directly interconnected, nor intended to be interoperated, does not obviate the fact that everyone understood that they would be co-located on electronic devices, would be subsumed under identical operating systems, and would be used together by individual consumers (and possibly malicious users) to achieve a variety of purposes (some neither envisioned, nor sanctioned by the companies). As such, they were then and continue to be, interoperable products. This case illustrates one of the subtle and more concerning difficulties associated with interoperability – once removed from a highly controlled setting, intentions do not necessarily have a lot to do with end use. Although the target of the hack in the illustration above states his "digital life was destroyed", fortunately he did not suffer bodily injury or death. Unfortunately, we have a decades' long legacy of what happens in higher stakes situations when failures in complex systems yield catastrophic results.

Safety critical systems can be counted upon to do remarkable things; they can also be relied upon to fail. Analyses from the Bhopal gas tragedy, the Challenger explosion, the Chernobyl and Fukushima Daiichi nuclear disasters and other human-made catastrophes demonstrate that these tragedies were not the result of linear or even a cascade of events. Instead, they can be better understood as the expected result of functional characteristics, such as variability, in complex sociotechnical systems [2]; they are, as Perrow observes, "normal" [3]. Is it hyperbole to conjure up tragic images of catastrophic death and disaster, when discussing SSU of interoperable medical devices? Perhaps, but we

* Corresponding author at: 7755 Soda Creek Rd., Pueblo, CO 81005, United States.
E-mail address: Libby@samaras-assoc.com (E.A. Samaras).
[1] http://www.samaras-assoc.com/contact.htm.

http://dx.doi.org/10.1016/j.jbi.2016.08.024

Nomenclature

Acronyms

AAMI	Association for Advancement of Medical Instrumentation
ASTM	American Society of Testing Materials
AMA	American Medical Association
FDA	Food and Drug Administration
HCP	Healthcare Provider
HDO	Healthcare Delivery Organization
HIMSS	Healthcare Information and Management Systems Society
HIT	Healthcare Information Technology
HL7	Health Level Seven International
HHS	Health and Human Services Administration
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Standards Organization
IT	Information Technology
MDI	Medical Device Interoperability
MPC	Multi-Party Computation
NIST	National Institute of Science and Technology
NIOSH	National Institute of Occupational Safety and Health
NWD	Needs, Wants, and Desires (i.e., Kano types)
OSHA	Occupational Safety and Health Administration
PnP	Plug & Play
SE	Systems Engineering
SSU	Safety, Security & Usability
US	United States

think not, as it already occurs with single medical devices used in isolation [4]. Evidence is mounting that the health care arena is far from immune to SSU interoperability-related issues. There are anecdotal accounts even today from hospitals regarding metric/imperial standard conversion interoperability problems, of the sort that contributed to the 1999 crash landing of the $125M Mars Climate Orbiter. While metric conversion errors and unsynchronized clocks will not cause a multimillion dollar collision in a hospital, to fragile children in need of precise dosing calculations based upon correct weight [5] and time interval, these mistakes can be deadly. Alarming signs include recent reports that the healthcare industry is highly vulnerable to SSU breaches, having been the most frequent industry target for cyber-security attacks in 2015, with nearly 90 million health records compromised at an annual cost of more than $6 billion [6]. These events should be red-flag warnings that a "patch & pray" [7,8] mindset in the medical device interoperability domain, will likely yield a bumper crop of complications, including serious injuries and death, significant liability for healthcare providers, healthcare delivery organizations and involved medical device manufacturers, as well as the resultant societal costs.

Patient stakeholders are reliant upon the intersection of technical, regulatory and business practices for the safe, secure performance and usability of interoperable medical devices. Unfortunately, these three have conflicting requirements and constraints that may undermine fundamental SSU. In this Viewpoint, we discuss the sometime harmonious, but frequently dissonant, context of regulatory, technical and business challenges to the development and performance of interoperable medical device SSU. We begin to just barely explore putative system-oriented solutions to these problems, while calling for restoration of historically-validated and scientifically-demonstrated strategies. In moving forward with medical device interoperability, it is imperative to understand impediments, draw from "lessons learned" wherever they may be found, implement proven strategies, and explore, refine or develop appropriately robust system-oriented methods to test and validate SSU of interoperable medical device systems. This clarion call seeks to shine a spotlight on the potentially serious SSU problems that may result when medical devices are cobbled together and applied to patients in what essentially will become, even with the best of intentions, uncontrolled experiments performed upon an unsuspecting, unconsented, and susceptible public.

2. Background

For more than fifty years, the rapid advancement and declining cost in computing capabilities and proliferation of the Internet have resulted in near ubiquitous reliance upon these technologies among industrialized nations, with connectivity a central fact in healthcare delivery [9]. This prompted collaborative global efforts to harmonize health information technology (HIT) over a more than three decades long commitment by the Health Level 7 [10], NIST, ASTM, ISO, IEEE, HIMSS and other governmental and non-governmental organizations worldwide [11]. As recently as March of this year (2016), the US Health and Human Services' (HHS) Center for Medical Interoperability announced two milestones involving major industry and health delivery organization groups' pledge to more open sharing of non-protected/non-proprietary health information, broader access for consumers and researchers, and implementation of federally-recognized interoperability standards [12,13]. Achieving this state of cooperation in US Health Information Technology (HIT) interoperability is unprecedented, long in coming, and the result of enormous national and international effort. Still, despite decades of work, full HIT interoperability is not fully realized; it is not reliable [14], and may remain only a hope for the future without better metrics [15].

Medical device development has been similarly impacted by the massive influx of computerization, with a somewhat parallel, albeit more guarded, impetus toward interoperability, especially where multi- or cross-vendor interoperability is concerned [16]. In a joint 2012 summit, the Association for Advancement of Medical Instrumentation (AAMI) and the US Food and Drug Administration (FDA) acknowledged that despite extensive effort on the HIT side, "little attention to date has been focused on the device side of that connectivity, especially as it relates to patient safety" [17, p. 3] and that healthcare lags behind other safety-critical industries in its pursuit of device interoperability. Major medical professional organizations, recognizing the promise of improved patient safety as well as potential for risks, have passed cautiously-worded resolutions in support of medical device interoperability (MDI). [18] Arguably because of the direct risk for death or serious injury [19] associated with the unintended failure related to command and control of MDI, as compared with its HIT counterparts, it is generally recognized that MDI "is an important concept that must be defined carefully and then pursued with equal care" [11, p. 1], with emphasis on "safety" and "intended purpose" [11, p. 10].

Nevertheless, significant work on MDI is underway, but not without controversy in approach and goals. As with HIT, many have called for open systems architectures, and the use, development, and adoption of consensus standards as key strategies toward achieving the goal of seamless MDI. "Plug and Play" [20], a term from early IBM PC days, as it applies in this context, is the "ability of medical devices, clinical systems, or their components to communicate in order to safely fulfill an intended purpose" [11, p. 7]. Dr. Julian Goldman, Director of the Medical Device Plug

and Play (MDPnP) Laboratory, a proponent of this approach to MDI, cautions device manufacturers to consider MDI as an integral and intended property from the outset rather than as an after-the-fact add-on [21]. Achieving the level of communication resulting in effective action, implied by the concept of medical device Plug and Play, requires a high level of dynamic interoperability that only comes about as a result of pronounced consistency and cooperation among all stakeholders [11, p. 13], which as we have seen in the evolution of HIT interoperability, may be decades long in coming, arduous, and difficult to realize.

3. Technical, business and regulatory challenges

Safety and security, and usability (SSU) are consistently recognized as essential Needs, Wants, or Desires (NWD) [22,23] for all stakeholders of interoperable medical devices. Significant technical, business and regulatory expertise and coordination must be brought to bear to achieve system SSU for all stakeholders. A systems view of safety for interoperable medical devices includes at a minimum assurances of patient (PT), provider (HCP), healthcare delivery organization (HDO), manufacturer (MFR) and societal (SOC) "safety" (physical, psychological, social, and financial), with system usability a critical component of both safety and effectiveness. Fig. 1 (left-side) illustrates a simple relationship between business, regulatory, and technical "pillars" that subtend interoperable medical device stakeholder SSU. Each pillar has its own or overlapping requirements with others (Fig. 1, right-side), including points of vulnerability and *stakeholder dissonance* [24] that can impact upon the SSU of interoperating medical devices. These important technical, business, and regulatory challenges that must be recognized and managed, are discussed in the following sections.

3.1. Technical challenges

The interconnection, interaction, and integration of interoperable entities can help solve existing problems in new and innovative ways. This paradigm is well-established in engineering, science, and the trades. Benefits are often the result of new combinations for collecting, processing, and controlling data and physical phenomena yielding new or increased efficiency and effectiveness. As we know from functionalist linguistic theory, they require appropriate input/output apparatus (morphology or technical interoperability), use of a common language with a shared vocabulary (syntactic interoperability), they must construct their messages in a manner that results in shared and unambiguous meaning (semantic interoperability), so they can successfully achieve their business objectives through effective and efficient workflows (pragmatic interoperability). The essential attributes of systems used by people in these workflows, especially people involved with healthcare, are safety (functional & physical), security (functional and physical), usability, reliability, maintainability, and affordability (see Fig. 2).

Interoperation will result in new, or previously unrecognized, hazards. Medical device interoperability will not stop with improving clinical workflow, data sharing with HIT, or connection between two devices. It will extend to multiple interconnected devices and the real-time utilization of data for control of ventilation, infusion, implants, and other safety-critical tasks. In contrast to traditional IT-centric solutions in healthcare (HIT), medical device interoperability poses a more direct and proximal risk of death or serious injury when safety critical devices are involved and learned individuals are not in direct, real time control of the process.

The generation of new hazards is well understood in the physical sciences and engineering. Engineers routinely construct by interconnecting hardware and software parts and components, eschewing to the extent possible *de novo* construction. They have tried and true principles and practices for managing both the process and the resultant hazards: engineering design control and engineering risk management. These have been practiced in various forms for centuries (if not millennia), began to be formalized in the early 20th century in systems engineering, and codified in formal standards in the mid-20th century. General Systems Theory [25] and Systems Engineering [26] teach multiple interacting subsystems give rise to system complexity and emergent behaviors. Emergent behaviors are sequelae of nonlinear, inhomogeneous, and non-commensurable interactions of system components that arise at their interconnections: the interfaces. They are, by definition, *a priori* unpredictable and nonobvious; they also are the theoretical basis for requiring complete and correct system design validations – because you cannot predict emergent system behavior from a study of the behaviors of the system components alone.

There seems to be broad advocacy for a "systems engineering (SE)" approach to interoperable medical device development [17,27,28]. At the same time, some proponents call for apparent shortcuts to the SE process, for example, by trying to "identify a pathway that will not require re-validation or re-clearance of the entire system" [28, page not specified]. Trying to streamline validation processes to foster distributed innovation may be laudable, but in our view this is misguided and likely dangerous.

Fig. 3 depicts interconnection of multiple FDA cleared or approved medical devices, which are presumed validated for safety, security and usability. A basic principle of SE is that the

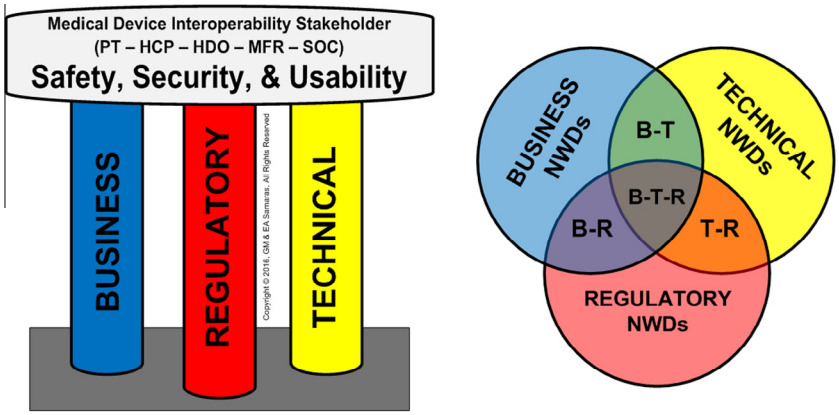

Fig. 1. Left: Three Pillars of Stakeholder Safety, Security & Usability. Right: Agonistic and antagonistic intersections of Stakeholders Needs, Wants, & Desires (B = Business; R = Regulatory; T = Technical).

Functional SAFETY	DEVICE HELPS (*INTENDED USE*)
Physical SAFETY	DEVICE DOES NOT PHYSICALLY INJURE (*BASIC SAFETY*)
Functional SECURITY	DEVICE PREVENTS DATA LOSS OR CORRUPTION (*INTEGRITY & CONFIDENTIALITY*)
Physical SECURITY	DEVICE CANNOT BE STOLEN OR DAMAGED (*DENIAL OF SERVICE*)
USABILITY	DEVICE REDUCES PROBABILITY OF ERRORS IN INTENDED USE BY INTENDED USERS
RELIABILITY	DEVICE FUNCTIONS AS INTENDED IN INTENDED ENVIRONMENT FOR INTENDED LIFETIME
MAINTAINABILITY	DEVICE REPAIRED IN REASONABLE TIME AT REASONABLE COST
AVAILABILITY	DEVICE ACCESSIBLE WHEN & WHERE IT IS ACTUALLY NEEDED
AFFORDABILITY	DEVICE SELLER & PURCHASER EACH OBTAIN ACCEPTABLE IRR (*REAL COST*)

Fig. 2. Medical Device Design Objectives (IRR = internal rate of return).

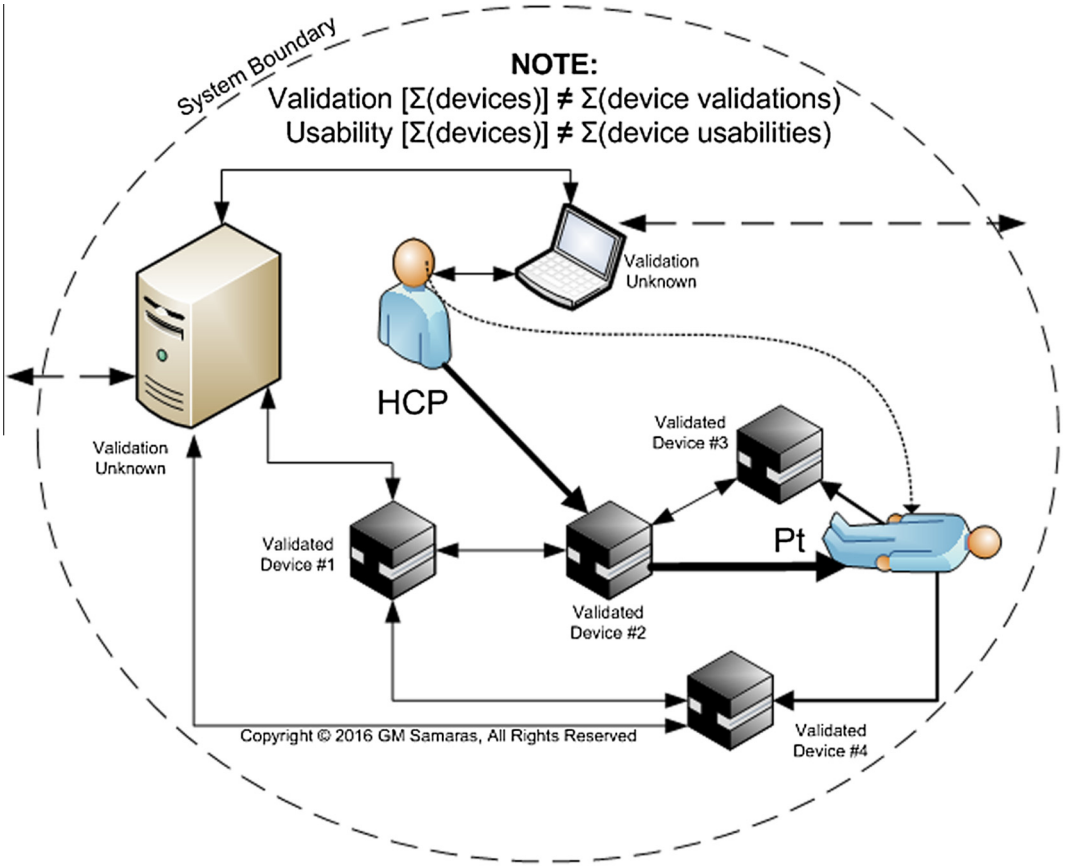

Fig. 3. Interconnection of validated components does not result in a validated system; only system validation of the interconnected system can achieve this.

validations of the components do not mean the integrated system of these components is validated. Emergent properties and new risks arise at the interfaces and can only be understood through validation of the integrated system.

Calling for a "systems engineering" approach that picks and chooses which SE principles and practices to employ is on its face contradictory [29,30]. "Systems engineering" without rigorous design verifications of risk controls and design validation of the nascent interoperable system(s) (a hallmark of the robust nature of the SE approach), is not systems engineering!

A shortcut in the SE process will, in all likelihood, result in failures to detect preventable system problems, or worse. Not only can and will data be corrupted or stolen, but behavior of a patient's ventilator, infusion pump, or implant could be modified in an unpredictable and unsafe manner (a not-so-implausible scenario given recent reports of ignition and locking hacker-related vulnerabilities among Volkswagen cars [31]. This can occur not only because of malicious actors. It can also occur as a result of subtle flaws in the design, implementation, and interaction of device hardware, software, and human factors engineering, especially for instances of "intended use" the original designers never considered. Subtle flaws might not be evident or troublesome for any one stand-alone device or with interconnection to any other single device. But, when a third, fourth, or nth device is recruited, the

result could be far worse, such as death or serious injury, because the combination of current industry practices, the existing regulatory paradigm, and proposed "short-cuts" cannot assure safety, security, or usability for complex interoperated medical device systems.

3.2. Business challenges

Perhaps to an even greater extent than was evident in efforts to harmonize HIT, a major methodological challenge in ensuring interoperable medical device safety and security will be to protect trade secrets and intellectual property without withholding requisite risk management and design information necessary to properly identify and mitigate potential hazards, as well as verify risk reduction efforts. Device manufacturers, like all business enterprises, are dependent upon returns on significant investments in research, development, and regulatory costs. As such, they legitimately may be guarded about existing revenue streams from their current, proprietary, single-vendor interoperable systems. "Best of breed" decisions made possible through vendor-neutral interoperability, while attractive for HDOs, may pose concomitant threats to manufacturers. These types of challenges are not limited to "across" businesses, but also "within" individual businesses, where we find closed subsystems or "silos" [32], which impede communication required for safe engineering practices and can compound the problem of MDI. Tradeoffs that consider these business issues will need to be balanced, but not at the expense of patient and HCP safety.

The push to demonstrate economic advantages of MDI is also an important business consideration for HDOs. They want assurances of safer, more efficient, effective, and reimbursable patient care before committing time and resources. By one estimate, billions of dollars may be at stake annually in the US as a consequence of direct and indirect cost savings from the widespread adoption of functional interoperable medical devices [33]. These projected savings are largely attributable to reductions in waste, but safety factors such as error reductions are also factors [33, p. 5]. The process of appropriately recognizing, earmarking, and equitably passing along medical device interoperability-related savings to manufacturers, HDOs, HCPs, and patients (as well as private and public payers), may be difficult without significant coordination and buy-in among all stakeholders [33]. As we discuss later on, any projected savings will likely be offset in part by reasonably foreseeable costs associated with the hiring of highly trained and experienced personnel necessary for the onsite configuration, upkeep, troubleshooting and validation of the new interoperable medical device systems.

3.3. Regulatory challenges

At the end of January 2016, the US FDA signaled its intention "to promote the development and availability of safe and effective interoperable medical devices" [34, p. 1] by issuing a Draft Guidance for industry. This heralds an era of potentially greater complexity for the Agency charged with regulatory approval and clearances of medical devices, without offering a satisfactory solution to the problem of risk control verification and system design validation for medical devices as they are introduced to the interoperable system. Unfortunately, the existing FDA regulatory model, like the medical device industry business models, is ill-suited to support promotion of safe and effective medical device interoperability. For example, the current FDA regulatory paradigm focusses on individual medical devices from individual manufacturers with approximately 90% of all devices never "approved" by the FDA, but rather administratively "cleared" for domestic marketing [35,36]. The Draft Guidance proposes continued reliance on this administrative clearance process, which will likely prove inadequate to the task of achieving safe and secure MDI, given that the risk level ascribed to any individual device will be altered through its interoperability with increasing or uncertain numbers of other medical devices [37], both individually and in combinations as interoperating systems [38]. And, as already discussed, the regulated community of manufacturers is organized as "closed" systems, rationally limiting the dissemination of their intellectual property and proprietary technology, but also radically limiting the availability of information to support risk control verifications and design validation of nascent systems of interoperating medical devices.

To further complicate the regulatory problem, HDOs currently use intermediaries and staff (clinical engineers, biomedical equipment technicians, and clinicians) to convert single medical devices into an interoperable medical device system. This behavior *de facto* turns the HDO into a medical device *manufacturer* under the current FDA regulations [39], yet there is no oversight of the "new" medical device systems that result. FDA's current Draft Guidance recommendation seems to encourage the HDO-as-manufacturer in its tacit promotion of this type of activity and its heavy reliance upon labeling of the interfaces, rather than rigorous compliance with design control and risk management of new, unique interoperable medical device systems [34]. This is an unprecedented approach in FDA regulation; it can be interpreted as the antithesis of regulatory control, insofar as it represents FDA's abrogation of its authority and mandate to assure medical device (not component) safety and effectiveness.

In 2014, FDA adopted the following cybersecurity definition: *"Cybersecurity - is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of* ***information*** *that is stored, accessed, or transferred* ***from a medical device to an external recipient****."* [40 p. 3, emphasis added]. Whereas, the Department of Homeland Security's cybersecurity definition is: *"The activity or process, ability or capability, or state whereby* ***information and communications systems*** *and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."* [41, emphasis added]. The FDA's modified definition of a generally-accepted nomenclature is an IT-centric, information-focused construction that effectively defines away all but information transfers to external recipients, eliminating unexpected and flawed communications and communications systems among two or more medical devices. Given this world view, it is not difficult to understand why the FDA might believe that mere labeling, which does not address critical issues of integrated system risk management and design validation, may be adequate to ensure the safety and effectiveness of interoperable medical devices.

It is important to recognize that from a human factors and ergonomics engineering perspective, the FDA recognizes the needs of the anticipated user in their draft guidance. What they do not explicitly recognize is the added complexity and implications for the user(s) in the enhanced use environment(s) engendered by the interoperating devices. Much as in the case of "alarm fatigue" that results from the uncoordinated layering of devices and their alarms (another, albeit rudimentary, interoperability problem) that overload already burdened users [42], if done haphazardly, MDI risks introducing a similar cacophony of safety–related regulatory and technical challenges going forward. Validating the usability of individual interoperable devices, or pairs of devices, or even the device with a representative of a class of interoperable devices [34, p. 9] again misses the point of systems engineering; the usability of each nascent system of devices must be subjected to the appropriate risk control verifications and system design validation, just like each individual medical device design (comprised of its interconnections of parts and components) must be verified and

validated. These usability-related issues add to the regulatory conundrum and raise formidable technical and business challenges in their own right, beyond those already identified, which we attempt to begin to address in the following discussion section.

4. Discussion and recommendations

Despite the important business, technical and regulatory challenges, as well as risks that have been identified already and those not-yet exposed, we still need, want, and desire interoperable medical devices for the enormous potential benefit they might offer all stakeholders. It is tempting to conjecture detailed interface information, such as the FDA's emphasis on labeling, can avert new or unrecognized hazards, but this likely will fall far short. It is also unlikely that the FDA can easily change its regulatory model [43] or that industry will alter its business models. We could just proceed with clinicians and HDO staff undertaking the responsibility (and legal liability) of interconnecting medical devices into systems on their own. This is certainly one interpretation of the FDA's current draft guidance with its reliance upon labeling the interfaces; but, labeling (a form of administrative control or warning) provides little assurance of operational safety and is ranked low in the hierarchy of prevention or risk control (e.g., according to OSHA, NIOSH, ISO). It is possible that systems integrators could undertake to study, test, and submit some combinations of devices for FDA clearance, but that would markedly reduce the extent of innovation at the front lines of healthcare. Understanding each individual device interface is necessary, but not sufficient (even in the presence of extensive harmonization), for risk identification, risk control verification, and system design validation of the (increasingly) complex interoperable medical device systems that will be inevitable. HDOs will likely move to improve their internal resource capabilities and expertise to begin to tackle the issues posed by interoperable medical devices within their specific setting, much as they had to establish and expand IT departments with the introduction and growth of computers, and to hire biomedical technicians and clinical engineers to handle the proliferation of electronic devices. The decentralized build-up of expertise among HDOs, while somewhat inevitable, is not a wholly comforting nor systemic resolution to the problem; it leaves far too much up to individual competence, or lack of.

So, how can we share the requisite engineering design information to perform system risk analysis and validation without revealing proprietary and confidential information? Currently in use in e-commerce, there is an approach, secure Multi-Party Computation (MPC), which is a cybersecurity method for secretly sharing confidential data, while analyzing and openly disseminating the results of computations on the combined data set [44]. It should not require altering business models or regulatory paradigms. Secure MPC is a relatively new subfield of cryptography developing protocols that allow various entities (individuals, organizations, etc.) to compute some function over a joint set of inputs, while maintaining the privacy of each entity's own inputs. So, using a simplistic example, if we wished to create an interoperable medical device system using five different devices (from five different companies), each device manufacturer could secretly share their risk analysis (in some standardized format) and the overall risk analysis would be computable without disclosing any single manufacturer's specific risk analysis. Whether MPC is robust enough for this task is unknown, but it is a methodological prospect worthy of pursuit. Manufacturers and the FDA could utilize Secret Sharing protocols that would permit secure risk management computation of any combination of interoperable medical devices. This would allow each manufacturer to view the resultant hazard identification and risks, without (in principle) any individual manufacturer's confidential information being disclosed. The MPC approach might prove viable for improved interoperability at the software and hardware level, but it would not resolve all obstacles. First, it will only be as good as the validity of the worst data set. Second, it does not eliminate the need for human factors and ergonomics (HF &E) validations at the front-line of care, which present additional and perplexing methodological challenges.

Conducting observation of the users in the front-line use environment is optimal for HF &E usability validations of MDI. But as we well know, this can be difficult, labor intensive and capricious in the highly dynamic, uncertain and complex socio-technical system that is healthcare. Further complicating that approach is that the healthcare system, must of necessity and by law, safeguards privacy. Efforts are ongoing and should be ramped up to systematize and simplify the process of human factors and usability testing of complex interoperable medical devices. This includes determining the appropriateness of virtual test environments (i.e., the graphical programming paradigm espoused by, among others, National Instruments and their LabView tool that is used extensively for decades in test engineering) [45], development and testing of use case scenarios and other types of simulations as is being done in the MD PnP Lab [46], and other approaches, including training of physicians, nurses and other HCPs using high-fidelity patient simulators in mock care units, and the use of avatars in "virtual" environments.

We also need more research and development of formal methods and practical principles of the sort advocated and studied by Thimbleby and colleagues at Swansea University, that would aid in designing and assessing complex adaptive systems, which could be valuable for interoperable medical device systems' study and testing [47]. Exploring appropriate systems-level frameworks, such as Hollnagel's Functional Resonance Analysis Method (FRAM) method for modelling non-trivial socio-technical systems [48] is another area worthy of investigation. The FRAM method could be applied either prospectively for non-linear risk assessments that may lend insight into otherwise unanticipated threats, or retrospectively for analysis of adverse events that occurred, associated with interoperable medical device systems.

Going forward with the design and development of interoperable medical devices, we cannot ignore fundamental safety principles, in favor of insufficiently tested "modern" approaches. The hierarchy of safety, wherein inherent safety or safety-by-design trumps the weaker safety strategies of engineering controls, personal protective equipment, or labeling and training, must be embedded in the systems integration processes. Redundant safety systems, fail-safe and fail-secure modes, and interlocks are important elements of system electrical, mechanical, and software safety that may be employed in interoperable medical device design. Systems engineering is generally recognized as one of the most robust tools we have in achieving interoperable (medical) device safety and it is the central underpinning of medical device development at the present. It is widely used in other high risk sectors, including the aero-space/aviation, automotive, nuclear and other safety-critical industries. Its principles and practices have also been codified in software engineering [49]. Undermining the SE process by creating short-cuts or removing critical steps in the process is a too risky proposition, unless and until another approach (such as mathematically rigorous formal methods [50]) can be proven time and again to be more reliable. Human factors and ergonomics should be considered early and often in the design and implementation phases of interoperable medical device development; all the human users (from all the different user groups) in the use environment are a critical, but often under-considered, component of system safety. Currently FDA, as well as international consensus standards (e.g. ISO 13485/14971) and industrial sectors (e.g. aerospace, automotive, etc.), require the implementation of rigorous

quality management systems that include design control and risk management for individual products. This includes thorough risk analysis, system verifications and validation, as well as post-market vigilance/surveillance activities, such as sentinel event (safety signal) recognition and corrective and preventive actions (CAPA), followed by re-validation of the proposed mitigations. It also requires the development of standard operating procedures and their adherence. These principles and practices have been developed over decades to prevent and appropriately respond to adverse events and to protect stakeholders – all the stakeholders; they should not be cast aside quickly in the quest for potential short-term benefits of MDI.

Safety and security are negative goals, manifested by the absence of harm. Failures to ensure safety and security can, on the other hand, be seen on a daily basis across all fields of endeavor and often involve limitations in usability; these failures are oftentimes attributed to "unintended consequences". That is not acceptable. With MDI, we can and must systematically anticipate hazards and control risks through effective prevention and mitigation measures at all phases of the interoperability lifecycle. We must also foster better and systematic reporting of adverse, sentinel events for their lessons learned and corrective action. Watering down the processes designed to maximize safety in the name of protecting innovation or trade secrets cannot be acceptable, but neither should we adopt processes that threaten innovation and intellectual property. We should anticipate that there will be substantive stakeholder dissonance between the regulator, regulated industry, deploying organizations, and providers/consumers of healthcare that will likely hinder the process of safe and effective MDI. Medical device interoperability will depend on recognizing areas of stakeholder dissonance and developing methods, procedures, and validated metrics to ensure reasonable safety, security, usability and evidence-based clinical effectiveness. Identifying the means for the successful sharing of engineering data to expose system integration risks and design flaws, before patients and providers are put at risk of harm, will be a critical step in resolving technical, business, and regulatory challenges to the safety of the interoperable medical device enterprise. Throwing out years of safety knowledge and well-established methodological approaches is not the solution; stepping them up and trialing them within in the context of modern methods, such as MPC Secret Sharing, graphical programming test methodologies, and formal methods that would help design and assess complex adaptive systems to meet the complex risks and challenges posed by medical device interoperability seems to us a more rational course of action.

5. Conclusions

There are pressing and predictable SSU vulnerabilities facing MDI. It will be incumbent upon biomedical informatics, with its interdisciplinary perspectives and methodologies, to confront many of them. This includes tackling the following vexing problems:

(1) How do we protect legitimate proprietary interests, while providing sufficient technical information that supports risk management and integrated system design validation of interconnected medical devices in our current regulatory climate?
(2) How do we systematize and simplify the study and validation of interconnected system usability of interoperable medical devices?

In our discussion, we identified a few modern approaches, that we believe are promising and warrant further investigation and research. Still it is our firm position that basic systems engineering and risk management principles and practices, which are not always in evidence in the pursuit of SSU MDI, must come first; without those as a minimum, we cannot even consider the more sophisticated methods.

Recognizing and resolving stakeholder dissonance - the explicit and implicit conflicts between the NWDs of different stakeholders as evidenced by errors, workarounds, and threats to patient and provider safety and organizational profitability - will be a central and iterative challenge for realizing safe, secure, usable, efficient, effective, and reimbursable interoperable medical devices.

In the final analysis, SSU MDI will be hard to achieve, especially given the dynamism that characterizes HDO environments. However, we cannot subscribe to the seemingly pervasive notion that MDI is such a unique and technological imperative that it warrants eschewing rigorous applications of proven scientific and engineering principles and practices. For their part, HDOs should act upon the Joint Commission's call for "high-reliability health care" [51], which will do much to contribute to SSU of interoperable medical devices at the local level. Over-reliance upon labeling, and seeking ways to shortcut validation of the entire system, especially in the absence of more robust techniques, does not bode well for success. Deviations from first principles threaten stakeholder safety and undermine the viability of MDI. Innovation in the absence of safety and security is not innovation. We agree with Mary Logan, President and CEO of AAMI when she recently warned of "Systems Overload":

> *. . .we need a greater scientifically focused commitment to a systems approach. . .before we have major disasters as a result of our cobbled-together solutions that we developed with the very best of intentions in our silos and comfort zones of expertize*
> [[52, page not specified]]

In balancing society's collective interest to benefit from MDI innovation against threats to individual safety and security, it will be important to keep in mind the generally-held primacy of non-malfeasance, "first, do no harm", which usually supersedes its bioethical corollary to "do good". Proceeding with caution, observing well-established safety, security and usability principles and system validation, followed by (or in concert with) careful testing of new approaches (and re-testing for reproducible results), is in our mind, the most responsible and most productive path to harvesting the potentially enormous benefits of MDI, while avoiding the potentially catastrophic harms.

Support

This project received no external funding.

Conflict of interest

None declared.

Acknowledgements

While the Viewpoint expressed and any inaccuracies contained are solely the authors, we would like to thank the peer reviewers for their thoughtful and constructive comments.

References

[1] M. Honan, How Apple and Amazon Security Flaws Led to My Epic Hacking <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/> (published August 08, 2012, page not specified, accessed 2/1/2016).
[2] E. Hollnagel, D.D. Woods, N. Levenson (Eds.), Resilience Engineering: Concepts and Precepts, Ashgate Publishing Co, Burlington VT, 2006.

[3] C. Perrow, Normal Accidents: Living With High Risk Technologies, Basic Books, New York, 1984.
[4] See FDA's MAUDE-Manufacturer and User Facility Device Experience <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Search.cfm> (last accessed on 8/19/2016).
[5] S.J. Bosker, A Weighty Mistake <https://psnet.ahrq.gov/webmm/case/293#> (published March, 2013, accessed 8/17/2016).
[6] S. Pettypiece, Rising Cyber Attacks Costing Health System $6 Billion Annually, Bloomberg 2015 May 7 <http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually> (as cited by ECRI Institute's infographic entitled: Cybercrime: The Healthcare Epidemic of the 21st Century. 2016 ECRI Institute: 2016).
[7] "Patch and Pray" is a Coined Phrase Used in Reference to Software Patching, See S. Berinato, Software Patching: Patch and Pray <http://www.csoonline.com/article/2116255/data-protection/software-patching-patch-and-pray.html> (published August 1, 2003, accessed 6/29/2016).
[8] "Patch and Pray" Technopedia Definition Describes Reactive Rather than Proactive Approaches to Cybersecurity <https://www.techopedia.com/definition/31040/patch-and-pray> (accessed 6/29/2016).
[9] I.J. Katlet (Ed.), Biomedical data, knowledge, and systems in contextI.J. Katlet, A. Verma, Singh (Eds.), Principles of Biomedical Informatics, Academic Press, 2014, pp. 579–581. e-Book.
[10] Health Level Seven International (HL7) Website <http://www.hl7.org/> (accessed 6/29/2016).
[11] Association for the Advancement of Medical Instrumentation (AAMI), Medical Device Interoperability, White Paper, Association for the Advancement of Medical Instrumentation, Arlington, VA, 2012 <http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/Summits/Interoperability/MDI_1203.pdf> (accessed 6/30/2016).
[12] Center for Medical Interoperability, HHS Announces Major Commitments from Healthcare Industry to Make Electronic Health Records Work Better for Patients and Providers <http://medicalinteroperability.org/hhs-announces-major-commitments-from-healthcare-industry-to-make-electronic-health-records-work-better-for-patients-and-providers/> (posted on March 1, 2016 and last accessed 6/29/2016).
[13] Center for Medical Interoperability, The Patient Safety Movement Announced 49 Medical Technology Companies have Signed the Pledge to Share Data <http://medicalinteroperability.org/the-patient-safety-movement-announced-49-medical-technology-companies-have-signed-the-pledge-to-share-data/> (posted on March 7, 2016 and last accessed 6/29/2016).
[14] J.D. D'Amore, J.C. Mandel, D.A. Kreda, A. Swain, G.A. Koromia, S. Sundareswaran, et al., Are meaningful use stage 2 certified EHRs ready for interoperability? Findings from the SMART C-CDA Collaborative, J. Am. Med. Inf. Assoc. 21 (2014) q060–1068, http://dx.doi.org/10.1136/amiajnl-2014-002833.
[15] American Medical Association (AMA), AMA and Other Medical Societies Call for a Change in Interoperability Measurements, 2016 <http://www.ama-assn.org/ama/pub/news/news/2016/2016-06-03-interoperability-measurements-ehr.page> (posted June 3, 2016, accessed 6/29/2016).
[16] To date, single vendor interoperability has been submitted and handled under the FDA's standard regulatory paradigm (21CFR §807.81).
[17] AAMI, Medical Device Interoperability: A Safer Path Forward. Proceedings of the AAMI-FDA Interoperability Summit, 2012 <http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/Summits/2012_Interoperability_Summit_Report.pdf> (accessed 6/30/2016).
[18] See for example, the AMA's resolution on Interoperability of Medical Devices, which acknowledges safety and medico-legal challenges and supports "... the proper balance to achieve optimum patient safety, efficiency, and outcome benefit while preserving incentives to ensure continuing innovation", AMA, Interoperability of Medical Devices H-480.953 <https://searchpf.ama-assn.org/SearchML/searchDetails.action?uri=%2FAMADoc%2FHOD.xml-0-4354.xml> (last modified 2015, accessed 6/29/2016).
[19] 21 CFR 803.3(w): "Serious injury means an injury or illness that: (1) Is life-threatening, (2) Results in permanent impairment of a body function or permanent damage to a body structure, or (3) Necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure. Permanent means irreversible impairment or damage to a body structure or function, excluding trivial impairment or damage".
[20] According to PC Guide's online archives, a form of "Plug and Play" (PnP) was first made available on the EISA and MCA buses, however, neither of them caught on until the term PnP was popularized in 1995 by Microsoft with its release of Windows 95 and the PC hardware designed to work with it, PC Guide Online Archives, Plug and Play <http://www.pcguide.com/ref/mbsys/res/pnp-c.html> (version date 4/17/2001, accessed 6/30/2016).
[21] J. Goldman, Solving the interoperability challenge, safe and reliable information exchange requires more from product designers, IEEE Pulse 5 (6) (2014) 37–39, http://dx.doi.org/10.1109/MPUL.2014.2355307.
[22] A.H. Maslow, A theory of human motivation, Psychol. Rev. 50 (1943) 370–396. <http://psychclassics.yorku.ca/Maslow/motivation.htm> (accessed 8/19/2016).
[23] N. Kano, Attractive quality and must-be quality, J. Jpn. Soc. Qual. Control (April) (2004) 39–48.
[24] Stakeholder dissonance (as opposed to cognitive dissonance), is a term for "...the conflicts between the Needs, Wants and Desires of different stakeholders. It is evidenced by errors, workarounds, and threats to patient and provider safety and organizational profitability". (p. 25) as defined by EA Samaras and GM Samaras in Using Human-Centered Systems Engineering to Reduce Nurse Stakeholder Dissonance, Biomed. Instrum. Technol. 44(s1) (2010) 25–32.
[25] L. von Bertalanffy, General Systems Theory: Foundations, Development, Applications, Braziller, New York, 1968.
[26] A. Chapanis, Human Factors in Systems Engineering, Wiley-Interscience, 1996.
[27] P.P. Reid, W.D. Compton, J.H. Grossman, G. Fanjiang, Building a better delivery system: a new engineering/health care partnership, Edited by Committee on Engineering and the Health Care System; Institute of Medicine; Institute of Medicine and National Academy of Engineering, National Academy Press, 2005 <http://www.nap.edu/catalog/11378/building-a-better-delivery-system-a-new-engineeringhealth-care-partnership> (accessed 6/30/2016).
[28] S.F. Whitehead, J.M. Goldman, Getting Connected for Patient Safety: How Medical Device "Plug-and-Play" Interoperability Can Make a Difference, Patient Safety Qual. Healthc., January/February 2008 <http://www.psqh.com/janfeb08/connected.html> (accessed 6/30/2016).
[29] G.M. Samaras, R.L. Horst, A systems engineering perspective of the human-centered design of health information systems, J. Biomed. Inf. 38 (1) (2005) 61–74.
[30] G.M. Samaras, An approach to human factors validation, J. Valid. Technol. 12 (3) (2006) 190–201.
[31] A. Greenberg, A New Wireless Hack Can Unlock 100 Million Volkswagens, Wired, 2016 <https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/> (last accessed 8/19/2016).
[32] G.M. Samaras, Medical Device Mechatronics Maturity, Medical Electronics Design Online Magazine, 2012 <http://www.medicalelectronicsdesign.com/article/medical-device-mechatronics-maturity-0> (accessed 6/30/2016).
[33] West Health Institute, The Value of Medical Device Interoperability: Improving Patient Care with More Than $30 Billion in Annual Savings, 2013 <http://docs.house.gov/meetings/IF/IF14/20130320/100535/HMTG-113-IF14-Wstate-SmithJ-20130320-SD001.pdf> (accessed 6/30/2016).
[34] Food and Drug Administration (FDA), Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf>2016 (accessed 6/30/2016).
[35] IOM, Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years, National Academy Press, 2011, p. 86. <http://www.nap.edu/catalog/13150/medical-devices-and-the-publics-health-the-fda-510k-clearance> (accessed 7/05/2016).
[36] G.M. Samaras, Exactly What Medical Device Innovation Are You Talking About? MD + DI Online, August 10, 2012 <http://www.mddionline.com/article/exactly-what-medical-device-innovation-are-you-talking-about> (last accessed 6/30/2016).
[37] A medical device is defined within the Food Drug & Cosmetic Act as "...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory..." <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm> (accessed on 7/5/2016).
[38] A related issue was raised in a joint letter from HIMSS and PCHA to Robert M. Califf, MD, Administrator of the FDA. In it, the signatories urged the FDA to align this draft guidance with the Agency's final guidance on medical device accessories "... such that medical devices will not be subject to an automatic determination that an accessory is in the same class as a device with which it works". However, it is important to note that their letter was referring to Medical Device Data Systems and not medical devices in general. See HIMSS/PCHA Letter to Robert M. Califf, MD, Administrator of the FDA, dated April 28, 2016 <http://www.himss.org/news/himss-joins-pcha-letter-fda-draft-guidance?ItemNumber=48338> (accessed 6/30/2016).
[39] 21 CFR 820.3(o). "Manufacturer means any person who designs, manufactures, fabricates, assembles, or processes a finished device. Manufacturer includes but is not limited to those who perform the functions of contract sterilization, installation, relabeling, remanufacturing, repacking, or specification development, and initial distributors of foreign entities performing these functions".
[40] FDA. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, October 2, 2014 <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf> (accessed 6/30/2016).
[41] National Initiative for Cybersecurity Careers and Studies, Cybersecurity 101: What is Cybersecurity? <https://niccs.us-cert.gov/awareness/cybersecurity-101> (accessed on 6/30/2016).
[42] The Joint Commission, Medical Device Alarm Safety in Hospitals, Sentinel Event Alert (50) (2013) (April 8).
[43] G.M. Samaras, A Perspective on Invention, Innovation, and Regulation of Medical Devices, MDDI Online and Magazine. 2011 (December 11).
[44] R. Cramer, I.B. Damgård, J.B. Nielsen, Secure Multiparty Computation and Secret Sharing, Cambridge University Press, Cambridge, England, 2015.
[45] For descriptions of these tools see National Instruments' <www.ni.com> (accessed on 7/5/2016).
[46] For a "walkthrough" of the MD PnP lab <http://mdpnp.org/lab.php> (accessed on 8/19/2016).
[47] See Swansea University webpage entitled: "Safer Human-Computer Interaction for Healthcare" <http://www.swansea.ac.uk/compsci/

researchandimpact/researchimpact/saferhuman-computerinteractionforhealth-care/> (accessed 8/19/2016, for a brief overview this research).
[48] See descriptions of FRAM - the FUNCTIONAL RESONANCE ANALYSIS METHOD for modelling non-trivial socio-technical systems <http://www.functionalresonance.com/> (accessed 8/19/2016).
[49] P. Bourque, R.E. Fairley, Guide to the Software Engineering Body of Knowledge, version 3.0, IEEE Computer Society, 2014 <https://www.computer.org/web/swebok/v3>.
[50] A. Mashkoor, J. Sametinger, Rigorous modeling and analysis of interoperable medical devices, in: Proceedings of the 2016 Spring Simulation Multi-Conference (SpringSim'16), Society for Modeling & Simulation International, pp. 800–807, 2016 (April) <https://www.se.jku.at/wp-content/uploads/2016/04/2016.rig_.modeling.pdf> (accessed 6/30/2016).
[51] M.R. Chassen, J.M. Loeb, High-reliability health care: getting there from here, Publ. Joint Comm. Milbank Quart. 91 (3) (2013) 459–490. <https://www.jointcommission.org/assets/1/6/Chassin_and_Loeb_0913_final.pdf> (accessed 8/17/2016).
[52] M. Logan, Mary Logan: Warning, Warning! Systems Overload, AAMIBlog, 2014 <https://aamiblog.org/2016/08/04/mary-logan-warning-warning-systems-overload/> (August 4, accessed 8/19/2016).