Cyber Security and Securing Subjective Patient Quality Engagements in Medical Applications: AI and Vulnerabilities

Marcus Wigan, *Senior Member, IEEE*

***Abstract*—Public policy arguments about the appropriate valuation of life in public policy have generally moved on from accounting resource costs to recognizing and including revealed preference valuations. In medical and public health, the valuation of the "quality" life experience over time (a very different concept) has focused on equivalents to an unconstrained life experience. The user perspective on these valuations is largely missing and has substantial implications for both individuals and organizations. As these summary measures are fundamental to current triage and assessment processes, they have considerable importance for individuals. Recognizing this, requires consideration of the number of different channels that can bias the assessment of individuals in specific circumstances when AI support is used, as a wide range of inferences from diverse data are then brought to bear and amplifies health data security scope and importance. These intermediate aggregate channel security vulnerabilities have not previously been highlighted, in spite of the importance attached to these summary measures in public health. The collision of totally individualized assumed impacts and end-user consequences are amplified rapidly by AI methods in support of decisions, and the security and privacy-if any is left—of individual medical AND life data are thus jointly at cyber risk. This article is a preliminary—largely gedanken- exploration of the results of combining these very different technical views and perspectives, and is intended to stimulate work that takes all these aspects into account.**

***Index Terms*—AI, cybersecurity, medical applications, patients, quality engagements, vulnerability.**

I. Introduction

THERE are many areas in public health that require some basis for assessing the impact of a treatment on an individual or a specific population. Simple measures of mortality are inadequate, and a measure of value is often needed for impacts that are less than the saving of lives. The most widely used single prospective measure of this combination of impact and value is the quality-adjusted life year (QALY). This attempts to combine the scale of an expected impact and the its value to the recipient. The two measures to be combined (likely impact of a treatment and the value placed on the outcome achieved) are simply noncommensurate, so there are—and will always be—disagreements on how they should be combined. Discrete observable biometric outcome measures are straightforward: the probability of mortality, or of securing a specific level of reduced blood pressure are two examples where biometric measurements are straightforward, and can then (from these standpoints) be expressed in terms of changes in quality of life, were the life to be lived unconstrained.

Manuscript received 18 May 2022; revised 24 June 2022 and 8 July 2022; accepted 8 July 2022. Date of publication 14 July 2022; date of current version 23 September 2022.

The author is with the Melbourne Conservatorium of Music, The University of Melbourne, Melbourne, VIC 3010, Australia (e-mail: mwigan@gmail.com).

Digital Object Identifier 10.1109/TTS.2022.3190766

II. Exploring QUALYs

Once the value to the individual is used as part of the weighting on the period of life gained under some or no constraints, interpreting the convincingly "independent" and "neutral" results becomes very messy, and complicated ways of trying to compare the assumed population utilities are often explored [1]. A simple example is useful. A person is prescribed a medicine that extends their life by three years, but at a quality of life (utility) of "0.2." The QALYs for this treatment would then be 0.6. If another treatment that cost twice as much produced 0.7 QALYs then that would be judged as inferior.

Clearly in a course of treatment over time there will be a steadily changing number of QALYs, adjusted continuously by the utility of life at each stage. None of this addresses the essential questions: what to the patient is the utility or quality of life? Population estimates and limited studies of specific populations over time are used instead of actually getting the value/preferences for each patient over the course of a treatment (tradeoffs of quality, pain, and life extension could in theory be used to assess this for each patient, but this could only be done in a data communications and feedback rich treatment environment). Sassi [2] covered calculations encompassing discount rates over time (and age) and the usual panoply of economic refinements once a basic approach has been adopted. In this case Sassi cites that this multiattribute utility model for QALYs can be used given the assumptions of a reliance on utility independence between life years and health status, constant proportional tradeoffs, and risk neutrality on life years. These are some of the uses of such prospective summary measures of patient experiences in various treatments.

Even in this succinct summary, it is clear that the characteristics and variations in taste and wider life contexts of individual patients are inevitably lost in prospective population-based perspectives.

III. What Happens When Real-Time Dataflows and Responses Are Added?

We next add a noncommensurate perspective: Once mass data flows and communications are encompassed, prospective assessments, and decisions can be substantially replaced or complemented by real-time updating, monitoring, and communication mechanisms, assisted by AI. AI takes many forms and can be used in many different medical and clinical applications [3]. A major distinction is needed as machine leaning (ML) is often assumed to be the only form of AI. The term "AI" extends much more widely to language understanding, rule-based systems, and many other approaches. ML is ideal for learning and reproducing complex behaviors, but is not so good at explanations for the basis of any changes in actions or behavior that might emerge from its operational (as distinct from exploratory) use in a continuing adaptive environment.

Once ML/AI is brought to bear, the scale of information and assessments can be an order of magnitude greater, and data acquisition and reduction can be massively improved. Using stated and revealed preference choice-based models of individuals then could easily become practical—even though involving a fundamental social shift between the medical decision and the personal preference models.

The rapid growth in the volume of real-time monitoring of biometric factors has been due to two accelerating trends.

1) Rapid voluntary take-up of biometric recording and storage devices (e.g., FitBit and Apple Watch), driven mainly by fitness tracking, but with a growing health awareness component. Already these include VO2, BP, and ECG measures-all with real-time connections.
2) Equally rapid growth in embedded medical devices, also with real-time communications. Pacemakers, and insulin pumps are just two widely used examples.

As these monitoring and real-time connections grow, as they will, they will change the basis of medical treatment monitoring and over time, the selection of treatment methods moving from historical population experience assessment-based data to include real-time patient feedback. Thereby a dynamically modified treatment protocol becomes practicable.

This begins—sand has already begun—with monitoring for emergency responses. But the protocol will (or could) also move to include patient experience feedback, thereby changing the nature of the treatment management interactions.

Let us assume that this occurs. What will be the problems? First, the choices and balances in the mind of the patent must have a greater weight—and affect the treatments given in increasing numbers of cases. Inevitably cost balances will change as well. Some patients will choose to suffer extreme losses in quality of life to survive long enough to see, a valued family marriage take place. In such cases the relevance of the QALY part of the aggregate multiattribute econometric measure will be undermined, as will the economic assessments of the treatment decisions.

It is arguable that this would be desirable ("patient-centered treatment") but please have mercy on those responsible for the public health policy and fund allocation processes: there are at present no ways in which such tightly personalized valuations could be measured, and if measured responded to, let alone aggregated to give policy clarity.

This is a research need in itself, and an inevitable consequence of the dual growth in data acquisition and data utilization in diverse environments—often unanticipated at the design stage. Such *gedanken* experiments as this present paper are invaluable in delineating unexpected aspects of roadmaps and future options analyses. That is, the specific objective of the present paper.

Embryonic steps are evident in the large scale and growing efforts in digital government. Ethical issues are not central to the current discussion, but are here enormously important in the development of any such integrated approaches in future. One result of this current brief *gedanken* exploration is that the author now intends to explore this area in future work.

It will be difficult for medical cultures to readily accept this as it changes the role of patients in their own treatment, and the conflicts between costs, treatment choice, and patients' better-informed perspectives will leave many areas of vulnerability to cybersecurity intrusions. The information collected will be valuable both to medical third parties—and to commercial interests. Such intrusions will therefore almost inevitably occur, given the growth in value of personalized data on an increasingly wider front. However carefully the information technology and communications (ITCs) aspects are designed, if the incentives are high enough security sooner or later will be proved inadequate.

IV. Advanced Care Directives

Advanced care directives (ACDs) [4] are increasingly being used to provide a basis for much better-individualized treatment tradeoffs as they explicitly include a range of personal value statements—and have some legal standing for them to be utilized. Dying with Dignity Victoria has a concise discussion if this aspect [5]. The use of ACDs both corrects and undermines the undifferentiated use of historically determined QALYs at end of life (QALY $= 0$), which is often a time of greatest medical expense, as well as the time of greatest need for patient preference buy in. ACDs are still not widely held and lack full legal backing at the point that they are needed. They are historically defined rather than a live real-time two-way engagement with the medical professions. While it is evident that they are not always followed. Real efforts are made by many governments to help individuals create them [6].

Quite how to handle these in a setting where QALYs may have been used to refine the selection of treatment polices and strategies is not yet entirely clear. However, the data provided in such a form has a direct effect on both.

This data is unequivocally personal, and produces almost exactly what would be needed to adjust patient-specific estimates of quality of life as they themselves (rather than a population they are assumed to belong to and be represented by) choose to accept it. It also provides a deep insight into the patients' orientations and values. Clearly these decisions are also in turn vulnerable to the prior information and perspectives and beliefs held each patient at the time they wrote their ACDs—and also subject to change over time, either by extra information or as a result of external persuasion or pressure.

A typical set of conflicted issues for physicians is summarized in [7].

A similar set of opportunities and problems arise related to the growth of precision medicine. When DNA data becomes a standard diagnostic tool on a routine individual basis or is integrated into AI methods of analysis and forecasting, it leads to well-known issues of the privacy and security issues particularly due to the highly individualized datasets automatically created. In addition, there is an expansion of risk in that a much wider connected community is now exposed to these potential security and privacy risks. As large sensitive datasets are required for full deployment of AI analysis, and the addition of individualized values to extensive biometric data substantially enhances the utility, evaluability—and sensitivity—of the resulting materials.

The roles of health insurance and government policies for treatment will be affected by both the fresh data and the AI interpretation modifying treatments. Aggregating these vastly enhanced data sets and dynamic treatment modifications will inevitably have fresh impacts across a wider frame than simply medicine, especially where privatized medicine is involved, and the responses could well instigate serious social issues that will need anticipatory actions to moderate.

This is particularly relevant for palliative care but applies equally well to a range of other major medical issues that extend over time and involve significant disability or pain (cancer being an obvious example). Valuation of the physical aspects in the measurement scales as currently used necessarily omits the life framework in which individual patient choices are made, although materially assisting the public health (economic) assessments of choosing to support or embark upon one treatment rather than another. Simply capturing the characteristics of pain or standardized constraints felt by a patient at different points in a treatment cannot capture the wider frameworks of individual patient (or prospective patient) priorities between different dimensions explored by the instruments used to get an aggregate quality-of-life profile over the life of a treatment.

"Quality" derived from a patient standpoint is currently necessarily derived from surveys over time on specific populations. A standardized way of measuring the "quality" of a patients' experience in illness or disability has emerged from several decades of extensive international collaboration, leading to the wide use of the EQ-5D-5L scale [8].

The five dimensions conventionally covered are:

1) mobility;
2) self-care;
3) usual activities;
4) pain/discomfort;
5) anxiety/depression.

Each of the dimensions has five levels. A visual analogue scale (VAS) is also available ranging from "the best health that you can imagine" to "the worst health that you can imagine."

The results are population dependent. Extensive studies have been done to determine patient—reported outcome utilities (to eventually assess state valuations), often using paired comparison explorations. A typical example is reported for a U.S. population by Craig and Rand [9], which pinpoints the QALYs for U.S. subpopulations. A real effort is expended to secure prospective assessments of the patient experience and quality of life via different treatments.

In your 'Advance care directive', you can include:

- A value directive
- An instructional directive.

A **values directive** is a statement of your values and preferences for your medical treatment. Your medical treatment decision maker will use your values directive to guide them when they make decisions for you.

Your medical treatment decision maker is the person with legal authority to make medical treatment decisions for you, if you do not have decision-making capacity (are unable) to make the decision(s).

An **instructional directive** is a legally binding statement in which you consent to, or refuse, future medical treatment.

Your instructional directive takes into effect as if you had consented to, or refused the treatment.

You can choose to complete **either or both** directives using this form.

Fig. 1. Values and instructions in ACDs.

ML/AI approaches could make considerable use of greater ongoing refinement for the patient as an active party. This is a task that can in many fields be considerably enhanced by ML methods of engaging in diverse and often noncommensurable datasets—and exploiting the rapid rise in two-way communication with patients—often automated—over the course of their treatment.

The different levels of pain, mobility etc., expected for the patient facing a range of treatments is not normally the way that these scales are used. These assessments provide for the individual with an expected profile and puts in their hands aspects of their treatment choices, as each individual has a wider range of contextual choices. A common end of life dilemma is "what will I put up with in terms of pain, constraints, etc., with in order to live to see a birth/marriage?"

Moving on from the descriptive data captured to build frameworks for prospective public health assessments to enhance the capacity to encompass the decision frameworks of the individual are in the best spirit of deploying ML/AI methods to encompass both individual variation and value frameworks, as far wider considerations can then be generated and offered. Critically, this development depends critically on large-scale two-way communications. That is, it depends on precisely where ML/AI methods can be deployed to assist both patient and medical perspectives. This in principle is a framework where both types of continuing choices could be handled.

Few if any communications systems can afford to ignore cybersecurity issues, and embedded medical devices clearly must have this as a major priority for the safety of the patient.

V. What Cybersecurity Issues Could Arise in Such Situations?

Many would be no different than those that arise in current medical situations, whether in intensive care or elsewhere. The difference is the real-time monitoring and exception identification and the feedback between the patient and medical professional with the choices then available with different categories of outcomes.

The expanding access to the data flows is already established, and growing. We must remember that continuous monitoring of ECG, BP, and heart behavior are all already readily captured by consumer instruments on a continuous basis. The wider access to these data flows—and the connections to treatment management—make all these information flows vulnerable. While for implanted instrument vulnerabilities to hacking for implanted instruments are already recognized [10]–[13]. In addition, patient-to-management communication and data flows, many automatically handled at both ends, are inexorably increasing.

A further critical and related *gedanken* experiment is the exploration of the capacity—let alone legal and ethical viability—of securing patient approval for what is already a complex set of tradeoff risks [12] in an already stressed environment for their decision making.

So while these medical data flows and devices are already recognized to be vulnerable (and require ML/AI assistance to reduce vulnerabilities), but the values and choices (if offered) of and to the patient are also potentially increasing. If these too are connected to existing data streams then the importance of protecting these flows rises sharply, and as decisions can be attached to them beyond the essential medical treatment factors, then these become even more sensitive and in need of protection.

ML/AI approaches can individualize micro and major decisions, but how much could (or should) be under the control of the patient? If any are, under the control of the patient then they need special communications protection in any ML/AI assisted environment, and the wide large-scale data resources chewed up by the ML/AI system also require special protection! Even if the only initial result was to be to raise the levels of engagement in treatment processes by patients, it would be a valuable early outcome.

In a survey of more than 300 clinical leaders and healthcare executives, more than 70% of the respondents reported having less than 50% of their patients highly engaged and 42% of respondents said less than 25% of their patients were highly engaged [14].

VI. Conclusion

Five key SocioTechnical issues emerge from this discussion as we move from the use of synthesized historical understandings to more dynamic interactions, and are the results of the *gedanken* experiment that this article documents. In addition to the further thinking already signposted by the author, these Socio-Technical issues are listed.

1) Changes in the balance between and engagements between medical treatment professionals and the patient.
2) Concerns over the security of the ever more sensitive data streams.
3) Vulnerability to unauthorized third party use of the ML/AI deduced characterizations of the patient.
4) Who "owns" which parts of this evolving and changing system?
5) What public health valuation frameworks will become needed and usable?
6) What ethical framework can be agreed across the wide range of disciplines involved to ensure a survivable social license?

References

[1] L. Prieto and J. A. Sacristán, "Problems and solutions in calculating quality-adjusted life years (QALYs)," *Health Qual. Life Outcomes*, vol. 1, p. 80, Dec. 2003. [Online]. Available: https://doi.org/10.1186/1477-7525-1-80
[2] F. Sassi, "Calculating QALYs, comparing QALY and DALY calculations," *Health Policy Plan.*, vol. 21, no. 5, pp. 402–408, 2006. [Online]. Available: https://doi.org/10.1093/heapol/czl018
[3] E. B. Sloane and R. J. Silva, "Artificial intelligence in medical devices and clinical support systems," in *Clinical Engineering Handbook* (Elsevier Public Health Emergency Collection). London, U.K.: Academic, 2019, pp. 556–568.
[4] "Alfred Health." [Online]. Available: https://www.alfredhealth.org.au/images/resources/patientresources/Instructions-forcompleting-the-Advance-care-directive-foradults-form.pdf (Accessed: Feb. 5, 2021).
[5] "Dying With Dignity Victoria." [Online]. Available: https://www.dwdv.org.au/honouring-patients-advance-care-directives/ (Accessed: Jul. 5, 2022).
[6] "Advanced Care Planning." [Online]. Available: https://www.advancecareplanning.org.au/ (Accessed: Jul. 5, 2022).
[7] "Australasian College for Emergency Medicine." [Online]. Available: https://acem.org.au/getmedia/0509a32c-26dd-455d-b7ce-14c9da77b711/1030-Anna-Holdgate-PRESENTATION (Accessed: Jul. 5, 2002).
[8] "EQ-%D-%L User Guide." EuroQuol Research Foundation. 2019. [Online]. Available: https://euroquol.org/publications/user-guides
[9] B. M. Craig and K. Rand, "Choice defines QALYs: A U.S. valuation of the EQ-5D-%L," *Med. Care*, vol. 56, no. 6, pp. 529–536, 2018.
[10] W. Kurisu. "Securing Connected IoT Medical Devices—Are We There Yet?" 2021. [Online]. Available: https://go.mentor.com/5gRnQ (Accessed: Feb. 17, 2021).
[11] B. Ransford *et al.*, "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists," *Pacing Clin. Electrophysiol.*, vol. 40, pp. 913–917, Aug. 2017.
[12] P. A. H. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices*, vol. 8, pp. 305–316, Jul. 2015.
[13] S. Anderson and T. Williams, "Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?" *Comput. Stand. Interfaces*, vol. 56, pp. 134–143, Feb. 2018.
[14] T. Davenport and R. Kalakota, "The potential for artificial intelligence in healthcare," *Future Healthc are J.*, vol. 6, no. 2, pp. 94–98, 2019.

Marcus Wigan (Senior Member, IEEE) received the D.Phil. degree in nuclear physics from Oxford, Oxford, U.K., in 1967, and has a multidisciplinary background, ranging through a number of disciplines since. The most recent postgraduate degrees include organisational psychology, IP law, applied ethics, international relations, and musicology.

He is an Emeritus Professor with Edinburgh Napier University in Transport and Information Systems, and currently an Honorary Fellow with the Conservatorium of Music, University of Melbourne, Melbourne, VIC, Australia. Sustained interests and publishing in ethics, surveillance, and privacy have continued during 21C during Honorary Professorships in Engineering, Sustainable Society, ICT, Social Inquiry, and Technology and Society at Melbourne, Swinburne, and Wollongong Universities. At the last check, he was still listed as a Visiting Professor with Imperial College London, London, U.K., in civil engineering in the transport centre. His current primary interest is focused on transdisciplinary issues affecting society though overlaps in engineering, ICT, governance and ethics: a Science and Technology standpoint.