CEN

WORKSHOP

AGREEMENT

CWA 17502

February 2020

ICS 11.020.10; 11.040.01; 35.020

English version

Privacy of monitoring technology - Guidelines for introducing ambient and wearable monitoring technologies balancing privacy protection against the need for oversight and care

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 17502:2020 E

Contents

Page

European foreword

CWA 17502:2020 was developed in accordance with CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – The way to rapid agreement" and with the relevant provision of CEN/CENELEC Internal Regulations – Part 2. It was agreed on 2019-12-02 in a Workshop by representatives of interested parties, approved and supported by CEN following a public call for participation made on 2019-06-07. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The project leading to this CWA has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No 690425.

The final text of CWA 17502:2020 was submitted to CEN for publication on 2020-01-14. It was developed and approved by:

— Technical University of Denmark / Henning Boje Andersen

— Technical University of Munich / Thomas Linner

— Schön Klinik Bad Aibling Harthausen / Barbara Schäpers

— Rigshospitalet, Copenhagen, Denmark / Maj Siercke

— IMSTA / Clare Harney

— Eindhoven University of Technology (TU/e) / Aarnout Brombacher

— Zorgbelang Zuid Holland (Patient representation) / C.A. (Kees) van Luttervelt.

It is possible that some elements of CWA 17502:2020 may be subject to patent rights. The CEN-CENELEC policy on patent rights is set out in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patents (and other statutory property rights based on inventions)". CEN shall not be held responsible for identifying any or all such patent rights.

The Workshop participants have made every effort to ensure the reliability and accuracy of the technical and non-technical content of CWA 17502:2020, but this does not guarantee, either explicitly or implicitly, its correctness. Users of CWA 17502:2020 should be aware that neither the Workshop participants nor CEN can be held liable for damages or losses of any kind whatsoever which may arise from its application. Users of CWA 17502:2020 do so on their own responsibility and at their own risk.

Introduction

New technological opportunities for monitoring daily living behaviours of frail citizens in need of care and oversight pose ethical challenges in terms of privacy protection. Sensors located in care receivers' homes or worn and interacting with their bodies to detect critical events and behavioural trends can not only improve early detection and care quality, but also reduce worries by frail elderly citizens and their families and care givers. At the same time, developments in demographics are leading to a significant increase in the number of frail older people living at home, while non-acute care is increasingly moving into people's homes. While regulations and guidelines are available for personal data protection and information security, there is no guidance on how to obtain an ethical balance between the duty of care and the need to respect the privacy and dignity of the people who are monitored.

The purpose of this document is to offer a practical, structured guide to achieve such a balance between the respect for privacy and the obligation to provide timely care. The focus of the guide lies on frail or vulnerable citizens and it is intended to be primarily of use for care organizations. It also may have value for families, technology developers and providers as well as regulators and authorities.

The guidelines describe a governance model and an adaptation of the informed consent process to accommodate the use of ambient and wearable monitoring technology in support of care decisions and treatment.

1 Scope

This CEN Workshop Agreement (CWA) gives guidelines for introducing, implementing and operating sensor monitoring technologies in the private homes of citizens who are in need of care and for the purpose of detecting critical events and trends.

The guidelines describe and exemplify the processes and procedures to support an ethically responsible balance between, on the one hand, respect for the autonomy and privacy of the citizens in need of care and, on the other, the obligation to provide quality care of typically frail citizens. The guidelines do not include issues of security or technical requirements for availability of information to relevant parties. The guidelines do not include management of or procedures for handling monitoring data.

This document contains

— a model for establishing an agreement on privacy protection between care receivers and care providers for the introduction, implementation and operation of ambient and wearable technologies;

— an adaptation of the informed consent process to achieve a balance between privacy and duty of care for the individual care receiver;

— examples of violations of privacy or neglect of duty of care.

The guidelines are intended to be of use for several stakeholders including the primary target group, care organisations. At the same time, care receivers (patients and citizens in need of oversight for health purposes) are the main focus, but will not be expected to be primary users of the guidelines. See Table 1 for other important stakeholders.

Table 1 — Target groups

Primary target group: — Care providers (public or private) who are responsible for delivering social care and health care to citizens **Secondary target groups:** — Care receivers (people who are in need of health and social care services) — Organisations representing care receivers and care providers — Families — Designers/developers/providers of monitoring technologies and services — Health authorities/regulators — Political decision-makers

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
privacy in healthcare
protection against unwanted access to personal information

Note 1 to entry: In ISO/TR 18638:2017, 3.26 “privacy in healthcare" is defined as the “right of an individual to keep oneself and one`s health information concealed or hidden”. In this document the focus is on the wish and right to not have personal data shared against the will of the care receiver, either explicitly or inadvertently.

3.2
care receiver
subject of care
subject of healthcare
patient, client
service user
healthcare actor with a person role, who seeks to receive, is receiving, or has received healthcare

EXAMPLE A treated patient, a client of a physiotherapist, each particular member of a target population for screening, each particular member of a group of diabetic people attending a session of medical education, a person seeking health advice.

[SOURCE: ISO 13606-1:2019, 3.1.7, modified — care receiver has been listed first as the preferred term, Note 1 to entry has been removed]

3.3
quality
degree to which a set of inherent characteristics of an object fulfils requirements

Note 1 to entry: The term "quality" can be used with qualitative adjectives such as poor, good or excellent.

Note 2 to entry: "Inherent", as opposed to "assigned", means existing in the object.

[SOURCE: ISO 9001:2015, 3.6.2]

3.4
information security
protection of information from (accidental or intentional) unauthorized access, use, disclosure, disruption, modification or destruction

[SOURCE: ISO/TS 21547:2010, 3.2.24]

3.5
informed consent
decision, which must be written, dated and signed, to take part in a clinical trial, taken freely after being duly informed of its nature, significance, implications and risks and appropriately documented, by any person capable of giving consent or, where the person is not capable of giving consent, by his or her surrogate decision-maker

Note 1 to entry: If the person concerned is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation.

[SOURCE: Directive 2001/20/EC]

3.6
autonomy
right to be self-governing agents

Note 1 to entry: In this document the term "autonomy" is used in the context of patient/citizen autonomy.

Note 2 to entry: This requires the right to decide on things of importance to oneself but also requires relevant information and a capability to understand the information; consider it in relation to personal values and decide accordingly.

[SOURCE: Bulletin of the World Health Organization 2008; 86:617–623]

3.7
security in healthcare
resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain

[SOURCE: ISO 28000:2007, 3.2]

3.8
care provider
healthcare provider
health provider
health service provider
healthcare service provider
healthcare actor that is able to be assigned one or more care period mandates

Note 1 to entry: The personnel of a healthcare organization that is a healthcare provider may include both healthcare professionals and others which participate in the provision of healthcare.

[SOURCE: ISO 13606-1:2019, 3.1.5, modified — care provider has been listed first as the preferred term, Note 2 to entry and Note 3 to entry have been removed]

3.9
ambient monitoring
monitoring by sensors in the environment of the conditions of a care receiver

Note 1 to entry: The data that are monitored can include and are not limited to vital signs, physical and social activities, body functions and behavioural data.

3.10
wearable monitoring
monitoring by body-fitted sensors of the conditions of a care receiver

Note 1 to entry: The data that are monitored can include and are not limited to vital signs, physical and social activities, body functions and behavioural data.

3.11
risk governance
actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented

Note 1 to entry: Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks.

[SOURCE: International Risk Governance Council]

3.12
risk management
systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring risk

[SOURCE: ISO 14971:2013, 2.22]

3.13
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989, 3.3.16]

3.14
empowerment
process designed to facilitate self-directed behaviour change

Note 1 to entry: In this document the term "empowerment" is used in the context of patient/citizen empowerment.

Note 2 to entry: According to WHO [SOURCE: World Health Organization (1998) Health Promotion Glossary. WHO/HPR/HEP/98.1. Geneva] in health promotion, empowerment is a process through which people gain greater control over decisions and actions affecting their health.

[SOURCE: Patient Educ Couns. 2010 June; 79(3): 277–282]

3.15
shared decision-making
process in which both the patient and physician contribute to the medical decision-making process and where care providers explain intervention measures and alternatives to patients and help them choose the option that best suits their preferences and their individual needs for care and security

4 Challenges and benefits of monitoring technologies

Seen from the perspective of the citizen, privacy is a core value, of equal importance as personal health, and is closely related to dignity and autonomy, but some reduction of privacy is normally accepted as a price to pay in order to obtain safety and confidence that care will be provided in a timely manner when needed. In contrast, if total privacy is maintained, there may be a constant worry that a sudden incident related to safety (e.g. a fall) may leave oneself helpless for an indefinite period, leading to disablement or even death - and similarly, a concern that one's family and close ones have the same worries.

Seen from the perspective of the care provider, respecting and protecting the privacy of the client is an important duty, and breaching this is ethically blameworthy and potentially embarrassing. Even if a breach does not violate any procedures or regulations, it is potentially embarrassing to be seen as being

instrumental (either inadvertently or negligently) in a privacy intrusion. This should be balanced against the potential harm to the individual care receiver of failing to exploit early warning technologies to alert of critical events, where again a breach of the duty of care can be ethically blameworthy, even though no procedure or regulation has been violated.

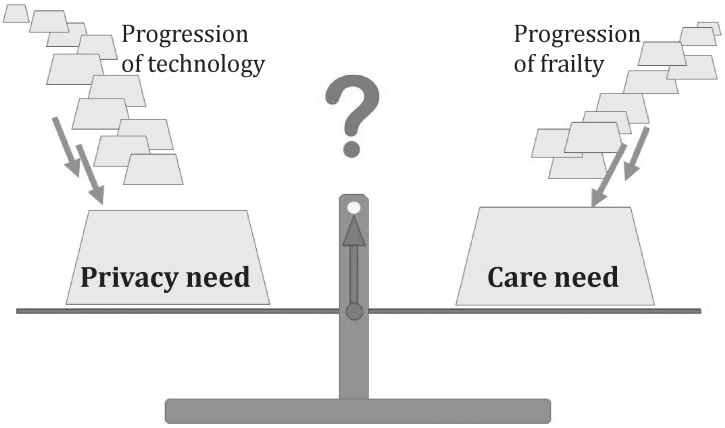

Figure 1 — Balance between privacy and care needs under the progression of technology and state of frailty

The concrete balance point between care and surveillance needs and the need for guarding safety and dignity depends on a complex of contextual factors that include recognition that the health state of the care receivers, and hence their care needs, may change over time, typically with increasing age, greater frailty and affliction by several chronic diseases. Similarly, the advancement of technology allows for ever deeper sensing and pattern recognition (Figure 1).

A main distinction with regard to the contextual factors is the question whether the offer of a technical monitoring system to support care is part of a health and social care system established by law where the duties are described and regulated or is a private commercial service regulated by only consumer protection laws. In both cases the first phase of application of the system and so the first period of validity of an informed consent should not exceed 6 months. After this time, a revaluation of the perception and experiences of the care receiver is necessary.

For the legally regulated scenario or use case a general transparent decision process with a generalized balancing of potential benefit and risks may become part of the regional or national governance process.

5 A risk governance model for informed consent

5.1 General

This document proposes to address the practical problem of achieving an ethically responsible balance between the duty to respect privacy and the duty of care in terms of a risk governance model that contains an adaptation of the well-established process of informed consent (Figure 2).

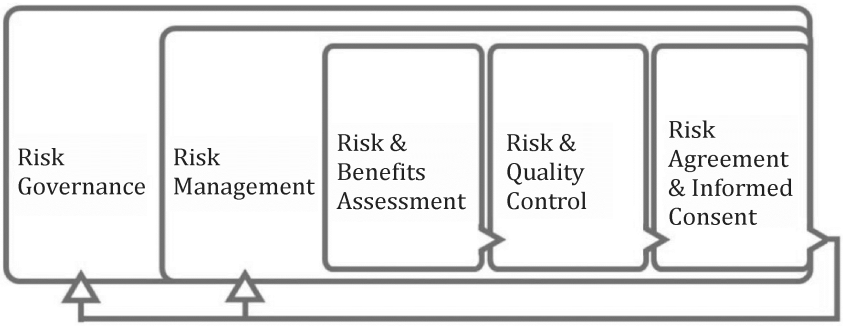

Figure 2 — Risk Governance model involving informed consent

5.2 Risk Governance

Risk governance is about how to identify, assess, manage and communicate risks; it contains the principles for transparency about how risks are dealt with – who decides, how to decide, and who is accountable. Principles of risk governance (outside of banking risks) are most often laid out with reference to the publication by the IRGC [15] and may be summarised as follows: "Governance refers to the actions, processes, traditions and governance, [which] includes the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken" [18].

While risk governance concerns the principles and policies for dealing with risks, the actual operational steps of managing the care challenge (the risk management process) is carried out by means of an informed consent process (Figure 2), thus, determining for each case an ethically sound balance between the duty of care and respecting privacy of the care receiver.

The individual steps in the risk management process should be updated at appropriate intervals.

5.3 Risk Management

5.3.1 General

The risk management process is divided into three phases. The initial phase for a given care provider organisation consists of securing an overview of the following inventory elements of resources, capabilities and services:

— the technical system:

  the system that provides monitoring including sensors, alarms and alarm setting, configuration, user interfaces for care receivers, care provider staff, installation, operation, maintenance, failure handling, responsibilities and roles;

— detectable events:

  the kinds of unwanted or critical events and trends that the monitoring system can detect and provide alerts and information about to care giver end users;

— care service responses:

  the types of responses and care services and service actions that can be delivered, depending on the information and alerts provided by the monitoring system.

In addition to the inventory of technologies and services, a description should be developed by the care organisation management of who may be eligible for monitoring, i.e., eligibility criteria for care receivers who may be offered different types of monitoring technologies and services.

5.3.2 Risk and Benefits Assessment

The overview of the inventory of technologies and services of the first phase should be accompanied by an assessment of risks, benefits and limitations of the three elements. In this phase it is important that care provider staff with both technical and care competencies participate and collaborate.

There are three types of risks associated with monitoring:

a) the risk of unwanted access to personal information (privacy violation);

b) security breaches (confidentiality; integrity of data; availability of data);

c) the risk of an inadequate or missing response which may arise either because of a technical failure or a care response failure (care that is wrong, inadequate, too late, or missing).

NOTE See ISO/IEC 27701:2019-08 and ISO/IEC 27001:2013-10 and ISO/IEC 27002:2013-10 for further information on security techniques and privacy information management.

Benefits associated with monitoring and the capture of unwanted events and trends are both psychological and clinical. The knowledge that care assistance will be alerted in case of a critical event may bring peace of mind to care receivers and their families as well to care staff. At the same time, monitoring may act as an early warning of health safety events that may progress to more serious conditions or death if the events remain undetected for longer periods.

A further benefit of monitoring technologies and services is their potential for empowerment of care receivers when they receive feedback from activity trackers, perhaps augmented with nudging, and when they experience progress in achieving behavioural goals.

5.3.3 Risk and Quality Control

Risk and quality control pertains to each of the three inventory elements listed at the beginning of clause 5.3 and are again divided into technical and care service issues.

Risk controls for the three types of risk are:

a) the risk of unwanted access to personal information (privacy violation) should be controlled by the risk agreement in the form of the informed consent process, described in clause 5.3.4;

b) security (confidentiality; integrity of data; availability of data) should be managed by the information security standards of all involved organisations;

c) technical risks of inadequate or missing alerts should be managed and controlled by the organisational units responsible for the technical system, whereas care response risks (care that is wrong, inadequate, too late, or missing) should be dealt with by the organisational unit responsible for care quality management.

NOTE For more information and guidance on care response see documents developed by CEN/TC 431 – Service Chain for Social Care Alarms.

5.3.4 Risk Agreement – Informed consent

The final step in the risk management process is shared decision-making involving the care receiver and care provider based on a dialogue between both parties about the risks and benefits of a monitoring service. It can be a considerable challenge for a care organisation to provide full and

understandable information to eligible care receivers for several reasons. First, care receivers may be weak and frail and may not have the mental strength or energy to process the information. Second, it requires both technical and care service competencies and sometimes legal ones to describe how privacy and security is ensured, and explain the kinds of unwanted or critical events that a monitoring system can detect. In addition, care providers should be able to explain how and what care will be provided when alerts or alarms are transmitted.

5.4 Informed consent adapted to privacy/care risks

5.4.1 General

In the informed consent process, risks and benefits have to be communicated realistically. The performance and impact of the monitoring system should be correlated with the environment and specific requirements of the care receiver. Therefore, the care receivers have to be informed about what they could expect when using the system. Performance and reliability should be central aspects if the system is designed to work with high-risk situations (e. g. detection of life-threatening conditions like cardiac arrhythmia). The care receiver should be informed about the level of safety for specific situations to allow decisions about actions in addition to the system actions.

5.4.2 Key elements of the informed consent process

The process of informed consent is traditionally tied to good clinical practice in the conduct of clinical trials on medicinal products for human use. The regulations governing participation in clinical trials should be adapted to the monitoring of health-relevant data including behaviours collected by monitoring technologies relevant to care and clinical decisions.

Informed consent can be described as granted permission or agreement freely given by an individual or their proxy decision-maker in full knowledge of any and all consequences. There are four main elements, in ensuring that informed consent is valid:

1. disclosure of information;
2. capacity of the individual or representative to make a decision;
3. comprehension of the information;
4. voluntary nature of the decision.

The need for care should not lead to any other release of personal and health data to the provider or other parties than what is minimally required to provide care.

5.4.3 Disclosure of information

In the informed consent process, risks and benefits have to be communicated candidly and realistically. Information about the performance and likely impact of the monitoring system should be correlated with the environment and specific requirements of the care receiver. Therefore, the care receivers have to be informed about what they realistically could expect when using the system. Technical performance and reliability should be central aspects if the system is designed to work with high-risk situations (e. g. detection of falls or life-threatening conditions like cardiac arrhythmia). The care receiver should be informed about which situations will trigger the system to alert or alarm care givers and the level of care response for the specific situations.

The provider should provide information about the components, structure, and handling of the system to ensure privacy, e. g. which care receiver behaviour will start, end, or change the format of data capture.

The provider should explain to the user specific functionalities and to what extent modularity is possible and useful. The care receiver should be informed about the data security status (personalised,

pseudonymised, anonymised), data format (clear pictures or body temperature, vital signs, test results, communication data, etc.), processing of the data (access by natural persons, processing by algorithms).

For all elements the care receiver should be informed of the risk of technical and care failure, and security breaches.

5.4.4 Capacity of the individual or representative to make a decision

The care provider has to ensure that the care receiver has the mental capacity to make the decision about the use of the monitoring system (capacity evaluation). When in doubt, the care provider has to seek the permission of the care receiver to contact other people who might be able to clarify the capacity status (e. g., family member, care giver, or physician). In case the care receiver has the legal status of diminished capacity, documents supporting this should be filed (in copy) with the informed consent document.

If a care receiver has the legal status of diminished capacity the information should be provided to the proxy decision-maker and, in addition, to the care receiver in a version adapted to the capacity limitations in question.

5.4.5 Comprehension of the information

Technical systems will typically address vulnerable people and are applied in a private and sensitive environment. They have complex socio-medico-technical functionalities and are subject to rapid development cycles. The resulting complexity makes it necessary to edit information (e. g. simplification and graphical representation) for the informed consent process to enable the care receiver to understand risks, benefits and limitations.

Care receivers with no diminished mental capacities may have difficulties in comprehending the complex information which therefore should be presented in a format adapted to the abilities of the person from whom consent is sought.

In the informed consent process, the care provider has to ascertain and document that all questions of the care receiver are answered and all information provided is understood.

5.4.6 Voluntary nature of the decision

The threat of refusal of care or the exaggerating of risks when not using the monitoring system shall never be used in order to coerce a care receiver into consent.

In case a care receiver withholds the consent to give access to data or expresses concerns about privacy issues, a realistic estimation of the risks (e.g., reduced care, safety issues, and/or limited communication to care giver) should be given. The provider should not exaggerate the risks and negative impact this restriction may cause, nor should the provider coerce the citizen to consent in full. Options without full data access (e. g., single modules, less invasive technical solutions) should be offered, when possible.

The care receiver should be informed about all circumstances affecting the interaction with the monitoring system, including implementation and operations.

5.5 Implementation of the monitoring system

The care provider should implement the system as described in the informed consent agreement. The functionality should be tested, stable, and full from the beginning. Especially in the early implementation phase, the care provider should be supportive of the care receiver. The care receivers and all persons who have access to their home should be instructed on the use, including checking of proper functioning and maintenance, of the monitoring system and remedies in case of failure.

Access to the home of the care receiver should be defined.

Shortcomings or disturbances of the system, e. g. based on environmental factors, may occur in the early phase. The necessary changes should be described to the care receiver, and added as information to the informed consent form to which the acceptance of the care receiver should be obtained.

5.6 The operational phase of the monitoring system

Informed consent should be revised whenever relevant changes of the health of the care receiver or the technical system or the care organisation make it necessary. This can change the balance between privacy and care (Figure 1) and require a more intensive care regimen. During the life-cycle of the system installation the care receiver should have easy and barrier-free access to multiple channels to contact the provider. If the status of the care receiver changes, e. g. a cognitive or physical decline, the provider should ensure that the care receiver is still aware about the nature, extent, and impact of the system. The appointment of a proxy decision-maker should lead to a new informed consent process with the proxy decision-maker. All risks and benefits have to be explained in relation to the actual situation of the care receiver.

Annex A
(informative)

Use Case Examples

A.1 Scenario Example 1

Patient details: "Muriel", 73 years old,

Health concerns: Generally healthy and mobile, requires blood pressure tablets, statins and aspirin.

Daily living and support structure: Lives independently in her own home in a small rural town. A son and other family members are living within a 15km radius of Muriel's home. General Practitioner is based 2km from Muriel's home.

Issues, concerns and actions: Muriel wishes to maintain independence. Her family is concerned about her living alone. Her son discusses home monitoring with the family practitioner who suggests a "panic alarm" and door sensors be added to Muriel's home. The family doctor explains to Muriel that the alarm may be used so that she can request immediate help in the event of an emergency and that sensors will be placed in the house to ensure her safety. Muriel agrees to installation.

Events: Muriel is feeling unwell and feverish, so she remains in bed after a poor night's sleep. She does not call for help as she knows that she is being monitored and feels that help will arrive if necessary. Her care provider is not alerted as sensors are active on external doors of the house only, and Muriel does not usually leave the house every day.

Outcome: Muriel develops sepsis and requires IV antibiotics and 14 days acute hospitalisation. Muriel's son realises that she thought the sensors would monitor her wellbeing as well as movements in and out of her home.

Comment: In this scenario, Muriel was not fully informed about how the sensors placed in her home worked. Muriel was under the impression that her sensors would alert her care provider if intervention was appropriate and so, she did not activate her panic alarm. Informed consent is vital to ensuring that the autonomy and wishes of the individual are respected, but also to ensure that the care recipient is aware of any limitations of medical devices placed in their home. *Respect of privacy, but neglect duty of care.*

A.2 Scenario Example 2

Patient details: "George", 76 years old

Health concerns: Recently diagnosed insulin dependent Type II Diabetes, mild obesity.

Daily living and support structure: Lives in his own home with his wife. Hospital outpatient appointment every 3 months and monthly General Practitioner (GP) visit. One adult daughter is based 90km away. General Practitioner is based 800m from George's home.

Issues, concerns and actions: George is not conforming to his prescribed diet and forgets to take his insulin as directed. His GP suggests implantation of a continuous glucose monitor that will alert George when he needs to take insulin. George asks a lot of questions about the implanted device and how it will impact his daily life. His GP assures him that it enables better self-management and will help him to identify when he has eaten foods that make him unwell. George feels well informed and agrees to have the monitor implanted.

Events: George is contacted by his GP as his glucose levels show he is not complying with his diet and treatment. He realises that his GP can access the data generated by his implanted glucose monitor and

he feels his right to privacy has been invaded, as the GP did not state that she would have direct access to his glucose levels via the implanted device.

Outcome: George feels that his autonomy to make his own decisions about his treatment is violated and requests that the device is removed.

Comment: In this scenario, while the GP answered all of George's questions, there was a failure to fully inform him of all aspects of how his device and associated data would be stored, shared and used. The onus is on the provider/prescriber to state all device and data usages and to ensure understanding is achieved as much as possible. *Invasion of privacy (duty of care).*

A.3 Scenario Example 3

Patient details: "Iris", 80 years old

Health concerns: Paraplegia, wheelchair user since age 51, otherwise well but becoming frail. No regular health appointments.

Daily living and support structure: Lives in her own adapted home independently. Iris attends a weekly social gathering organised by the local community care centre. Each week, she is collected in an adapted bus by staff from the community care centre, who briefly check her wellbeing and enquire about any additional health or living needs. Iris deeply values her privacy and consistently states that she is managing fine and that she doesn't need any help.

Issues, concerns and actions: Iris is offered an occupational health home visit regularly, which she declines. Staff at the care centre, concerned for her wellbeing and noticing increasing frailty over time, respect her privacy and do not intervene further. Instead, they offer Iris a personal alarm button so that she may contact care providers if needed. Iris accepts this compromise.

Events: A year later, Iris quite suddenly feels very unwell at home and presses her personal alarm button. The battery in her device has failed and nobody is notified.

Outcome: Iris suffered a poor physical outcome following a stroke in her home and subsequent delay in receiving clinical care. She loses her independence and is relocated to an assisted living facility.

Comment: In this scenario, there was a failure to balance privacy with duty of care and to update care provided as frailty progressed. Due to the difficulty in persuading Iris to accept the device originally, staff had been reluctant to intervene further, choosing to respect her wishes over a duty to ensure the panic alarm was functional at regular intervals and that her care needs were provided for. *Failure to update balance between privacy and duty of care.*

Bibliography

[1] ISO 14971, *Medical devices — Application of risk management to medical devices*

[2] ISO/TR 18638, *Health informatics — Guidance on health information privacy education in healthcare organizations*

[3] ISO/IEC 27701:2019-08, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[4] ISO/IEC 27002:2013-10, Information technology — Security techniques — Code of practice for information security controls

[5] ISO/IEC 29100:2011-12, Information technology — Security techniques — Privacy framework

[6] AVEN T., RENN O. Some foundational issues related to risk governance and different types of risks. *J. Risk Res.* 2019

[7] BARRY M.J., EDGMAN-LEVITAN S. Shared decision making--pinnacle of patient-centered care. *N. Engl. J. Med.* 2012 Mar 1, 366 (9) pp. 780–781

[8] BEAUCHAMP T.L., CHILDRESS J.F. *Principles of Biomedical Ethics*. Oxford University Press, USA, 2001

[9] ENISA (European Union Agency for Cybersecurity) (2018) Guidance and gaps analysis for European standardisation — Privacy standards in the information security context

[10] ENISA (European Union Agency for Cybersecurity) (2015) Security and Resilience of Smart Home Environments — Good practices and recommendations

[11] FALAGAS M.E., KORBILA I.P., GIANNOPOULOU K.P., KONDILIS B.K., PEPPAS G. Informed consent: how much and what do patients understand? *Am. J. Surg.* 2009, 198 pp. 420–435

[12] FIELDS L.M., CALVERT J.D. Informed consent procedures with cognitively impaired patients: A review of ethics and best practices. *Psychiatry Clin. Neurosci.* 2015, 69 pp. 462–471

[13] FLITE C.A., HARMAN L.B. (2013) Code of ethics: principles for ethical leadership. Perspectives in Health Information Management/AHIMA, American Health Information Management Association, Vol. 10. Winter.

[14] HEGDE S., ELLAJOSYULA R. Capacity issues and decision-making in dementia. *Ann. Indian Acad. Neurol.* 2016 Oct; 19 (Suppl 1) pp. S34–S39

[15] IRGC (INTERNATIONAL RISK GOVERNANCE COUNCIL). (2005) Risk Governance: Towards an Integrative Approach, White Paper No. 1. Geneva: IRGC.

[16] NIJHAWAN L.P., JANODIA M.D., MUDDUKRISHNA B.S., BHAT K.M., BAIRY K.L., UDUPA N. et al. Informed consent: Issues and challenges. *J. Adv. Pharm. Technol. Res.* 2013 Jul; 4 (3) pp. 134–140

[17] NISTIR 8228 (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, National Institute of Standards and Technology Interagency or Internal Report 8228

[18] AVEN T., RENN O. Some foundational issues related to risk governance and different types of risks. *J. Risk Res.* 2019. DOI:10.1080/13669877.2019.1569099