UiO : Faculty of Law
University of Oslo

Health safety & privacy: A case study on welfare technology in municipal eldercare

Legal challenges related to the municipality's acquisition and use of state-of-the-art technology

Candidate number: 6006

Submission deadline: 31.05.2021

Number of words: 17748

Table of contents

1 Introduction

1.1 Context

Modern healthcare services face increasing pressure with a workforce that lacks needed capacity and resources to combat emerging challenges of an ageing population. In the European Union (EU), the ratio between people aged 20-64 and those above 65 [1] will increase significantly in the coming decades. [2] Following a steady increase from 29% in 2010 to 34% in 2019, the ratio will rise to 59% in 2070. [3] Consequently, the number of working-age people for every elderly will drop from four to less than two persons in working-age. The significant jump in the share of an elderly population requires more skilled health personnel, facilities, and medical aid to care for the elderly prone to mental and physical diseases. By 2050, Europe's labour force will be reduced to half of what it is today. [4] Already in Norway, 1 in 5 quit their jobs within their first ten years as active nurses. [5] While reasons for this vary, surveys display crucial factors: disproportionate amounts of workload, low wages, and an overall sense of inadequacy amongst professionals to provide a high moral, ethical standard towards patients. It is a significant issue if the healthcare service becomes ill-equipped to meet the basic needs of a higher number of citizens who reply on its functioning. In this environment, technological innovations are a colossal asset in supporting workers and safeguarding safety, dignity, and integrity. Welfare technology is relevant to the above problem as both public organisations increasingly use ICT services as an essential part of the organisation and strategy in the healthcare sector. By fostering innovation in welfare technology, healthcare providers can assist patients to live safely in their homes. Repetitive and heavy tasks previously conducted by workers can be transferred to technical devices such as detections sensors and software applications that allow remote monitoring of patients. In effect, the healthcare service can become more effective and leave contested prioritisations and decisions regarding a

---

[1] Referred to as the EU's demographic old-age dependency ratio.

[2] European Commission (EC), "The 2021 Ageing Report: Underlying Assumptions and Projection Methodologies," (2020).

[3] Ibid.

[4] Marie and Jørgensen Langskov, Tina., "Technology and the Welfare System – a Discussion Paper," in *The National Political Conference on Welfare Technology* (Copenhagen, Denmark: European Commission (EC), 2008).

[5] Statistics Norway (SSB), "1 Av 5 Nyutdanna Sykepleiere Jobber Ikke I Helsetjenesten," https://www.ssb.no/helse/artikler-og-publikasjoner/1-av-5-nyutdanna-sykepleiere-jobber-ikke-i-helsetjenesten.

patient's life and death up for a discretionary evaluation done by a professional. Still, implementing technology in a person's home and private bedroom is an invasive measure that poses several risks of a disproportionate level of interference with a person's right to privacy and requires a proportionality assessment. On the other hand, technology may be the least invasive measure, as computers are based on binary numbers and pre-defined parameters instead of human flaws and emotional prejudice. Moreover, any scepticism and resistance amongst individuals to the use of technology will undoubtedly affect and steer how private and public organisations manage and operate systems. [6]

1.2 Relevance and purpose

There is no uncertainty about the numerous benefits of adopting technological systems and solutions to streamline heavy workload and repetitive healthcare services. The main issue pointed to in this paper stems from the high demand and pressure on the public healthcare service to tackle an increase in elderly patients and users and the actors involved in procuring state-of-the-art technology to offer necessary high-quality services to its citizens. The elderly may have poor ICT skills to understand its unforeseeable implications and effects; there is a high risk that these will form part of a marginalised experiment group in a project on innovative welfare technology without understanding the detrimental effects this entails. Incentives from the municipality and private companies in economic gains could also lead to a lack of indispensable human resources and skilled health personnel. This thesis aims to investigate the RoomMate technology implemented as part of public healthcare services. RoomMate as a measure aims to reduce and prevent harm to patient health and safety by means of a sensor and software application that detects critical situations the elderly patient finds him/herself in. This thesis' objective is to critically assess the utility and significance of the municipality's decision to utilise technology along with a unique responsibility to provide healthcare services that serve the interest of citizens.

[6] Michela Cozza et al., "Future Ageing: Welfare Technology Practices for Our Future Older Selves," *Futures : the journal of policy, planning and futures studies* 109 (2019).

1.3 The significance of GDPR [7] Article 25

As one of the new provisions since the GDPR entered into force, Article 25, "Data protection by design and by default" (DPbDD), offers an attempt to oblige data controllers to preserve privacy-related interests as key goals when defining system requirements. The provision could be a source of the growing global discourse on built-in privacy and security. Although new as a legal requirement under the GDPR, the concepts of security and privacy by design are not new. *Privacy by design* (PbD) was introduced by Cavoukian in Northern America in the 1990s and decided at a privacy conference in 2010. [8] The concept evolves around seven main principles to ensure the privacy of data subjects to «gain personal control over one's information» and for organisations to gain «a sustainable competitive advantage». [9] *Security by design* was developed in the 1970s and defined to a varying degree by various actors such as the Organisation for Economic Co-operation and Development (OECD) and ENISA. [10] Suppose these philosophies are valued as a legal requirement. In that case, a potential outcome is a possible decrease in personal data breaches and minimised access to confidential information that could limit the damage caused in such an event. These concepts are critical in a healthcare context and the development of welfare technology. One example is the RoomMate technology, developed with a PbD approach from the start of the design process. The system consists of a 3D sensor and an application to visually monitor patients and automatically alert care providers when a patient has fallen or otherwise risks health damage. As of May 2021, the private limited company RoomMate AS offers a complete alarm system, including passive and active notification units and a remote supervision solution. [11] Their service has been subject to projects piloted across municipalities in Norway, Sweden, and Denmark. Upon completing the acceptance test, RoomMate won the tender with Oslo municipality and is to be deployed and in operation as part of healthcare services.

---

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[8] Ann Cavoukian, "Privacy by Design - the 7 Foundational Principles," (Information & Privacy Commissioner Ontario, Canada, 2009).

[9] Ibid.

[10] Willis H. Ware, Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security.

[11] RoomMate.no, "Roommate Systemet – Et Komplett Sykesignalanlegg," https://vimeo.com/525444389.

1.4 Research questions

I. In what way are public healthcare providers such as Oslo municipality obliged to ensure information security and privacy requirements before, after and during new purchase and deployment of innovative ICT solutions?

II. How does RoomMate serve as an example of innovative welfare technology that satisfies DPbDD?

III. What are the risks and opportunities of using welfare technology that involves a combination of camera surveillance, sensor technology and audio recording? Can such technology conflict with patients' rights to healthcare and employees' rights in the workplace? If so, what can be done, and by whom, to mitigate these risks?

1.5 Methods

A study of the municipal healthcare services procurement of welfare technology offered by a private ICT supplier was valuable for illustrative and practical purposes to address the many ethical challenges and regulatory hindrances faced with the secure adoption of innovative technology to assist care workers. This paper will examine the municipality's measures to satisfy relevant regulatory requirements in legislation and industry norms to ensure patient's rights and effective services and resources in the healthcare sector. Methods include assessing provisions in relevant EU Acts and Directives and the Norwegian regulatory framework in health law, privacy, and data protection in the context of welfare technology used to provide municipal eldercare services. A particular focus is the concept of DPbDD as a regulatory mechanism to balance competing interests to patient safety and health on one side and privacy on the other.

This paper will study two leading organisations, RoomMate AS, a private limited company and the Oslo municipality's Agency for Health (Helseetaten). This will include a critical assessment of the actions, duties, and obligation arising from the municipality's procurement and involvement in the lifecycle and stages of development and deployment of the RoomMate technology in the main chapters 3 and 4.

Methods used to conduct research:

- **Desk research and document review -** Consisted of assessing relevant Norwegian legal instruments with binding force such as the Patient and User Rights Act (PURA) [12] and the municipal Health and Care Services Act (HCSA) [13] and EU/EEA relevant Regulations and Directives, as well as case-law. As the GDPR applies to all sectors of society and is incorporated into Norwegian law by the Personal Data Act [14], the Regulation has been highly relevant to assess research questions. Soft law instruments such as standards, codes of conduct, official guidelines, reports, and media coverage have been invaluable in evaluating regulatory policy issues in the highly complex subject-matters healthcare and ICT. Methods used to conduct research include scholarly work such as books and journal articles, guidelines, reports, and media coverage. The policies and opinions of the former Article 29 Working Party 29 (WP29)[15]and the European Data Protection Board (EDPB) [16] have been valuable to interpret the legal framework on European data protection, [17] as well as publications by the European Union Agency for Network and Information Security (ENISA). Still, it is worth highlighting that these bodies do not create binding pieces of law. AS their role is solely advisory, reports and opinions are worthy of critical scrutiny.

- **Interviews** – Two sets of interviews were performed to gather knowledge-based qualitative data: One with the CEO in RoomMate AS. A second separate interview was conducted with three employees in the Agency for Health (Helseetaten) in Oslo municipality as part of the Welfare Technology Section and the public procurement of automatic safety

[12] Lov 2.juli 1999 nr. 63. Lov om pasient- og brukerrettigheter (Pasient- og brukerrettighetsloven) [The Patient and User Rights Act - PURA].

[13] Lov 24. juni 2011 nr. 30. Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven) [The Health and Care Services Act - HCSA].

[14] Lov 15.juni 2018 nr. 38. Lov om behandling av personopplysninger [The Personal Data Act].

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, 0031–0050, Article 29(1).

[16] Prior to the EU Cybersecurity Act entered into force 27 June 2019, ENISA gained permanent mandate as an independent center of expertise to foster cooperation and policymaking on cybersecurity within the EU.

[17] Until 25 May 2018, the WP29 was the advisory, independent body on issues of data protection and privacy prior to the application of the GDPR.

alarm system and digital supervision solution. [18] The municipality has executive powers derived from legislation and governmental steering.

The goal of the first interview was to gain insight into the business operations, design and development process to grasp experiences, hindrances, gains and overall interests and considerations encountered by **RoomMate AS**. The interview format was unstructured, with open-ended questions adapted to welcome experiences of the interview object. The second interview with employees in **Oslo municipality** was valuable to obtain necessary information on the extent to which the healthcare service sets out requirements for privacy and information security in the use of innovative and invasive welfare technology to demonstrate compliance. The interview was set up semi-structured with a general schedule of questions sent via e-mail before the interview.

Both interviews lasted for one hour and were made possible by the digital video conference platform Microsoft Teams, to comply with current regulations due to the COVID-19 virus and avoid being a burden on the national healthcare service subject to long-term and increased pressure. A potential weakness of the thesis is the lack of information from health personnel and patients/users. Due to ongoing restrictions on physical meetings in Oslo from autumn 2020 to spring 2021, it was not feasible to obtain interviews with patients, users, and personnel subject to the RoomMate solution. These experiences would have been precious in addressing the user needs, expectations and acceptance of technology and its use. However, this paper is mainly concerned with the responsible parties, the ICT supplier, and the municipality's role as custodians of health information about citizens. Nevertheless, official reports and preparatory works, studies and surveys have been the primary sources of patients and user experiences of welfare technology as its intention depends on their acceptance.

Legislation and literature in the fields of data protection and information security are often focus-oriented and general. This means that the municipality usually has a high degree of autonomy to decide measures appropriate for implementation based on a context-dependent assessment and evaluation of risks. There is no suspicion that any actors are in breach of rights and

[18] Helseetaten, "Velferdsteknologi," (https://www.oslo.kommune.no/getfile.php/13313507-1549878854/Tjenester%20og%20tilbud/Helse%20og%20omsorg/Fag%20og%20kompetanse%20-%20helse%20og%20omsorg/Velferdsteknologi%20%20brosjyre.pdf).

obligations to secure ICT systems and manage sensitive information about patients. Nevertheless, this factor should be raised as the interview method also involve weaknesses of high proximity to the interview subjects. [19] To critically assess the information from the two sources has been essential as qualitative data reflects subjective opinions and bias that should not be taken at face value. [20] The information has still been beneficial to retract practical issues based on qualitative data gathered during the interviews and the written requirement specifications from the municipality.

1.5.1 Delimitations

This paper analyses the primary obligations following the GDPR as incorporated [21] into Norwegian law by the Personal Data Act. [22] Therefore, this thesis will exclusively deal with national and supranational laws relevant to Norway, with a clear focus on data protection, information security, and privacy pertinent to natural and legal persons in a healthcare context. It will attempt to define key roles and responsibilities in the context of welfare technology in municipal eldercare. In doing so, interpret and apply Article 25 to assess its legal impact on data controllers and processors in a practical scenario. While several principles and challenges can be shared across borders, this thesis is written from the perspective of Norway as a welfare state. As a member state of the EEA, Norway is part of the EU single market and enjoys the four freedoms of goods, services, and people and capital. [23] Also, local health authorities across borders and municipalities could share similar experiences with the case study. Still, key factors such as access to resources, labour force, geographical distances and other socio-economic differences come into play and vary from one municipality to another. Moreover, interviews conducted as part of this research were in Norwegian and translated into English. Translations are thus a result of the author's interpretation and do not reflect the opinions of others.

---

[19] Dag Ingvar Jacobsen, *Hvordan Gjennomføre Undersøkelser? : Innføring I Samfunnsvitenskapelig Metode*, 3. utg. ed. (Oslo: Cappelen Damm akademisk, 2015).

[20] Ibid.

[21] The EEA Act implements the main part of the EEA Agreement into Norwegian law.

[22] The Personal Data Act.

[23] Agreement on the European Economic Area (The EEA Agreement), Article 1(2).

1.6 Structure and outline

This paper is systematised in three main sections. The purpose of this introductory chapter is to set the context with the main issues and research questions to assess to what extent the obligation of DPbDD can be a mechanism to safely balance the interest of patient health and safety against consideration for privacy self-determination, and integrity. Any key definitions and abbreviations to fulfil the paper's objective is covered as part of this chapter.

Chapter 2 will define welfare technology and the detailed functions of the RoomMate technology, highlight relevant advantages and pitfalls of using an automatic warning system by sensor technology, including images and audio components. Further, relevant sources, key roles and responsibilities of data controllers and processors will be established following the requirements specifications stipulated by the municipality.

Chapter 3 will assess how identified risks can be managed by applying specific requirements and legal obligations upon data controllers and processors. The role and responsibility of the municipality will be the primary addressee to assess what technical and organisational measures necessary to mitigate risks and safeguard the individual's privacy, security and access to justifiable healthcare services.

Chapter 4 will analyse the strengths and weaknesses of deploying solutions such as RoomMate by municipal health providers and explore the significance of DPbDD as a mechanism to balance competing interests of patient safety and health against privacy considerations. Lastly, it will assess whether the current law serves as a helpful tool to assist municipal healthcare services and protect elderly patient's fundamental rights and freedom.

Lastly, Chapter 5 will summarise the main arguments discussed in this paper before concluding remarks and critical points.

1.7 Key terms and definitions

1.7.1 Healthcare

While the term *healthcare* symbolises a close relationship between the provision of health and care services, this paper will focus mainly on issues relevant to the concept of *care*, particularly eldercare as a service offered to elderly patients and users.

This thesis focuses on the decentralised provision of *public* healthcare services as a publicly managed and funded sector offered by local authorities at the municipal level. Norwegian health legislation distinguishes between *patient [pasient]* and *user [bruker]*. In a care context, this group is also commonly referred to as *residents*, as they reside in nursing homes to receive continuous healthcare services. Still, many *residents* live in their private homes.

Recipients and *providers* of care services will be used to avoid ambiguity with similar terms in respective fields of ICT and healthcare. Also, a clear distinction between patients as recipients of services and the healthcare service is needed. The large group of patients, users, and residents in private or nursing homes will subsequently be referred to interchangeably as *patients* and *recipients* of healthcare services.

Healthcare providers include a broad spectre of actors working in healthcare, including health personnel and the municipality and top leadership across the public and private healthcare sector. The terms *worke*r, *health personnel*, *staff* and *users* will interchangeably refer to employees in the healthcare service who work closely with patients daily.

1.7.2 ICT and data protection

Users are to be understood as users of ICT services. *Users* encompass more broadly general users and refer explicitly to healthcare workers in the workplace, administrators, and all roles given access to manage the RoomMate technology. An *organisation* includes legal actors, the municipal healthcare agency and the RoomMate company, also referred to as *supplier* of ICT services and equipment.

The regulatory definitions in the GDPR will be used, such as the definition of *personal data* as "any information relating to an identified or identifiable natural person [24] (*'data subject'*)". [25] The *data subject, controller* and *processor,* are the addressees of the relevant data protection framework, where data subjects earn substantial data protection rights. [26] For this paper, a data *controller* is a public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data. [27] A *processor* can be any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [28] These roles have varying obligations to ensure that the processing of personal health data is performed in a lawful, fair and transparent manner in protecting data subjects' rights. [29]

[24] GDPR, Article 4 (1) para. 1.
[25] GDPR, Article 4(1).
[26] GDPR, Chapter 3 (Art. 12-23).
[27] Ibid, Article 4 (7).
[28] Ibid, Article 4 (8).
[29] GPDR, Article 5(1)(a).

2 Requirements in the municipality's procurement of welfare technology

Digital transformation involves changing the fundamental ways organisations solve their tasks with the help of technology and is a pivotal goal to enhance the effectiveness and quality of healthcare to provide citizens with the best services possible. A known problem in Norwegian eldercare is the ongoing fall problematisation. A typical scenario is that the elderly patient is at home alone, fall and unable to call for help. This is a critical situation that could involve imminent danger to the safety and health of the individual. Historically, this problem has resulted in extreme demand for healthcare services that providers are unequipped to tackle due to the workforce's lack of force. If medical assistance is not offered immediately, consequences can be fatal as the worst possible outcome could result in losing lives. Consequently, the social welfare system also suffers from economic loss due to a need for supplementary resources. [30]

2.1 Welfare technology

Welfare technology as a concept stems from welfare states originating in Denmark. Welfare technology can be offered as practical assistance and knowledge to maintain, contribute and increase the feeling of safety, activity, participation, and independence for a person of any age who has or is at an increased risk of having/developing a disability. [31] Welfare technologies may be additional tools to assist healthcare providers in providing care services and must satisfy legal requirements as part of the provision. This could be a combination of hardware and software components such as sensors, monitoring devices and electronic medication dispensers. The offer in eldercare ranges from traditional passive safety alarm systems to advanced and increasingly automated means in the shape of global positioning system (GPS) applications and sensors to log and alert health personnel in certain activities or the lack of action. The idea of a welfare state entails that most citizens have great trust in governmental bodies to ensure egalitarian ideas and interests. The Norwegian state has a positive obligation to protect personal integrity. [32] In major life-changing events, such as the birth of a child, citizens of a welfare state expect the social system to act as a safety net and provide aids of economic and

[30] NOU 2011:11, "Innovasjon I omsorg" [Innovation in care], 30.
[31] Ibid, 99.
[32] The Norwegian Constitution, Section 102, para.2.

social significance, especially in times of crisis, such as the loss of a job or unexpected sickness where the offer of health and care services are vital to protect yourself. The use of welfare technology may be inferred partly from paternalism, the basic idea that parents know what is best for their child. The notion of paternalism denotes a relationship of control and a justification for this. In this context, the idea of welfare paternalism could also justify the municipality, as a public authority, making choices on behalf of the elderly patient to control their actions for their benefit from health and safety. By implementing welfare programs, laws, or policy to improve citizens' well-being, the government actively acts in the interest of citizens, often without their consent and even against their will. [33] Dworkin establishes three aspects of defining paternalism, namely an interference with integrity without the individual's permission that is beneficial for the individual. [34] In many ways, a municipality has a legitimate need to collect vast amounts of personal data about its citizens regarding health, economy, or other private or familiar relations to protect individuals and society. But the interference shall never be arbitrary and thus requires a proportionality and necessity test.

2.2 The RoomMate technology

The solution was initially a fall prevention alarm. Over time, advanced functionalities have been added, and events now include a range of activities and inactivates of the care recipient. Examples are falling, sitting, moving around from the bed, bathroom, leaving or entering the room. [35] Today, RoomMate AS sells the 'RoomMate safety sensor', a passive detection unit that monitors the individual and the room where installed. It automatically sends a notification or alarm as soon as it detects the individual is exposed to a critical event. [36] RoomMate is a type of welfare technology that can assist elderly patients, maintain, contribute, and increase patient safety, autonomy, privacy, and integrity. The target group consists of long and short-term patients largely dependent on valuable healthcare services.

---

[33] Douglas MacKay, "Basic Income, Cash Transfers, and Welfare State Paternalism," *The journal of political philosophy* 27, no. 4 (2019).

[34] Edward N. Zalta, "Paternalism," (Stanford, CA: Stanford University, 2013); Gerald Dworkin, "Paternalism," *The Monist* 56, no. 1 (1972).

[35] RoomMate.no, "Roommate Anonymisert Tilsyn Og Pasientvarsling," https://www.roommate.no/roommate/.

[36] Ibid.

RoomMate can be defined as a *passive safety alarm system* and *remote supervision solution* to assist healthcare providers, recipients and next of kin. The purpose is to detect the activities of the patient. Examples are a fall or moving in and out of bed. The authorised user (e.g., healthcare professional, a close relative, or a guardian) can conduct remote supervision via the RoomMate application on a smartphone, tablet or PC (*fig.2.2.)*

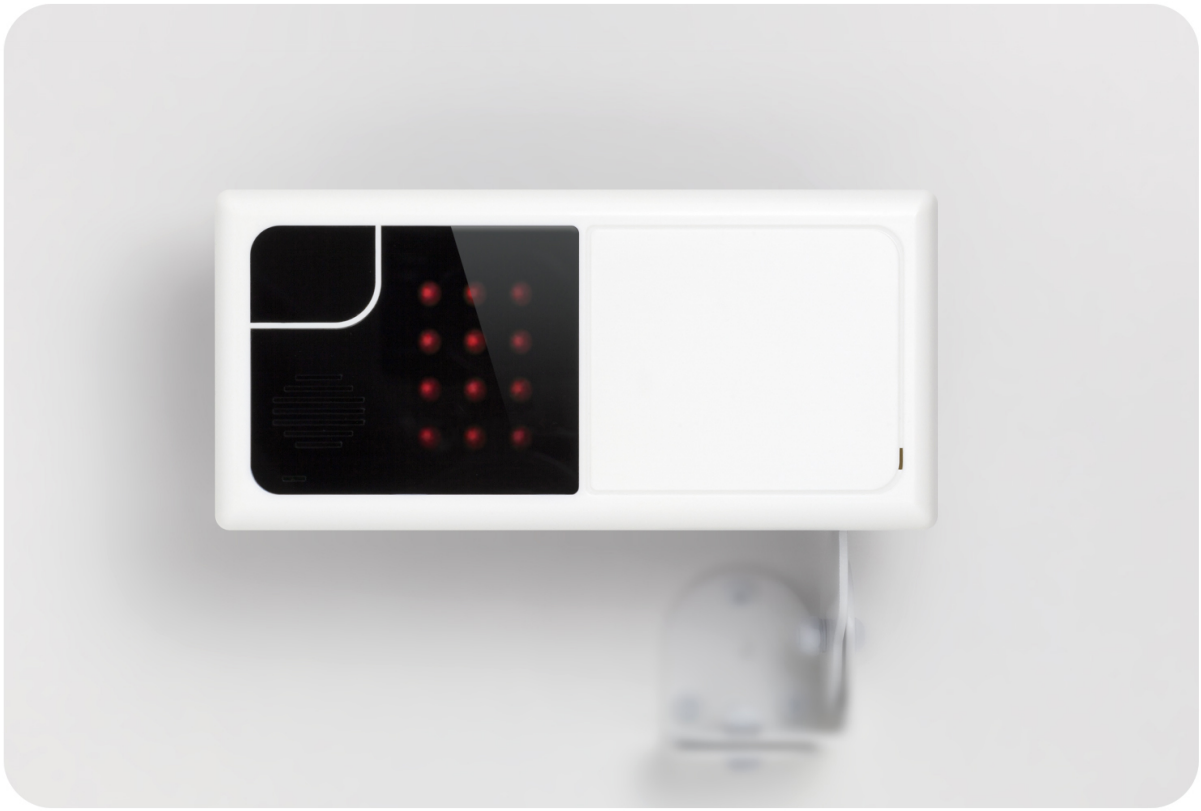

Fig. 2.1. RoomMate sensor system

2.2.1 Three-dimensional (3D) sensor technology

Based on emitting IR light and analysing the reflected light signal, the depth-sensing Room-Mate technology measures and calculates distances across the room, recognising humans and objects within its field of view. [37] For example, when a person enters, the sensor will detect and follow the person if they move within the sensor's range and area of view. [38]

Images coming from the sensor appear on the connected device as this is part of a system consisting of an IR light-based 3D sensor (*fig.2.1.)* that generates three types of images. The

[37] TK RNJ, "Roommate, Installasjonsveiledning, Rev D," (RoomMate AS, 2018).
[38] Ibid.

computer images are analysed, which forms the basis for computer graphics used for monitoring care recipients in their bedrooms.

Fig.2.2. User interface on connected device (phone, tablet or PC)

The application gives an overview of all rooms where different symbols (*left-hand side)* signalise the status of real-time events for every patient in rooms where RoomMate is installed (*fig.2.2.).* Once installed and configurated, RoomMate automatically sends alerts and alarms without requiring the care recipient to do any action or carry any equipment. The worker logs in to the device to perform supervision of the care recipient in each room. The worker is notified of critical events such as a fall and can keep track of the patient/user movements via the connected device.

2.2.1.1 Images

A built-in computer analyses the images from the 3D sensor in the hardware [39] for automatically alerting workers of critical situations. Planned, spontaneous, and event-based

[39] See *fig.2.1.*

supervisions can then be done remotely. The sensor can show three different images. [40] One option is a detailed image (*fig.2.3.).* The second is a more indistinct image; nevertheless, a possibility to recognise the individual is present.

Fig.2.3. Detailed image. [41]

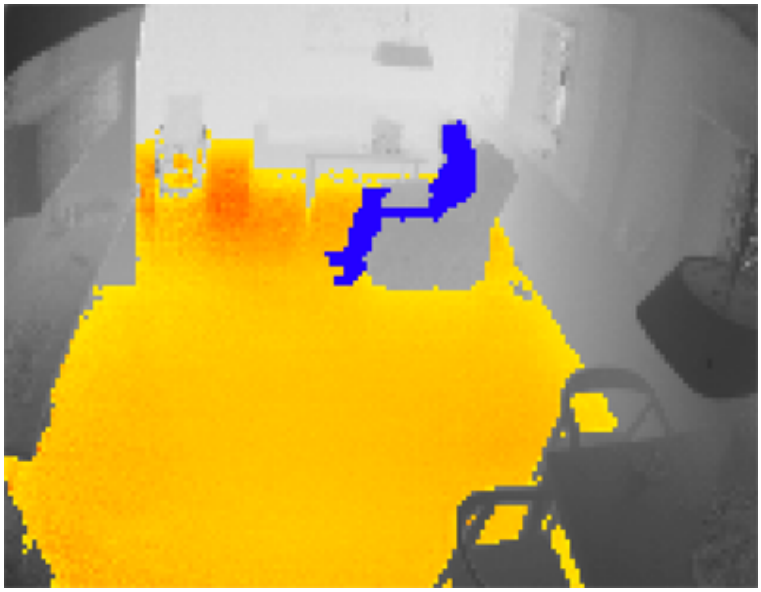

Fig 2.4. Infrared image, person (in blue) sitting in chair.

[40] RoomMate.no, "Roommate Anonymisert Tilsyn Og Pasientvarsling".

[41] Pictures re-used from RoomMate.no with permission.

The third option is an infrared image (*fig.2.4)*, where it is impossible to identify details of the individual's face and body. It is nevertheless possible to see the physical shape and follow the activities and movements of individuals moving around the room.

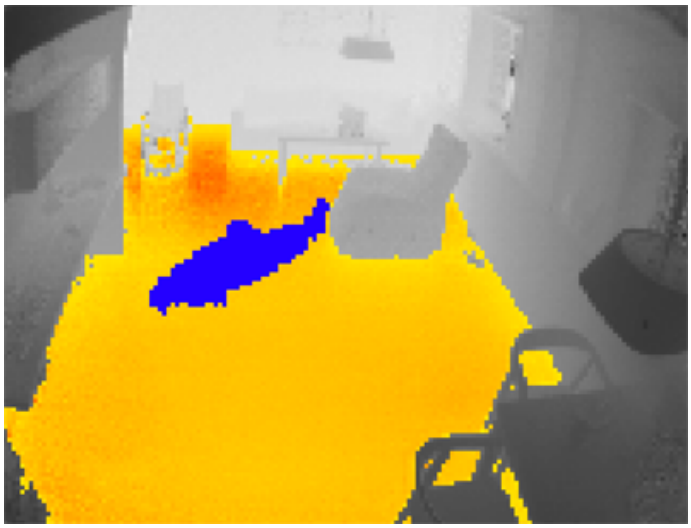

Fig.2.5. Infrared image, person (in blue) falls to the floor.

RoomMate automatically detects a patient who falls and lies on the floor (*fig.2.5)* to notify the alarm recipient, often being available healthcare personnel on duty.

2.2.1.2 Audio

The sensor contains a speaker and microphone. The audio function can be activated directly in the browser, and the worker may contact the patient for a two-way dialogue. If an alarm goes off, the worker can communicate with the patient to assess the seriousness of the situation. Listening can occur with and without distorting the sound in the room. This way, the system can detect loud noises without hearing what is said by persons in the room. The techniques used by RoomMate to avoid linking images and audio components to the individual patient will be analysed in Chapter 3 of this paper.

2.2.1.3 Installation and technical limitations

The physical deployment and installation of the RoomMate sensor could affect and reduce the privacy risks for patient and health personnel. If the sensor is installed above the door, it might be unable to detect the faces of those entering the room. This could be a measure to safeguard the privacy interests of individuals better. However, a blind spot underneath the

sensor makes a person detected as they are a certain distance from the sensor. [42] The installation is also affected by the functions enabled by the system for each patient, such as whether the remote supervision functions should be activated and fall alarms and out-of-bed alerts are also included. [43]

The sensor is fixed in the top corner of a wall in the patient's room in nursing homes, private homes, and similar institutions/homes. [44] The sensor must have in its field of view the space of the patient and sufficient floor area as it uses this as a reference. This would often be in the patient's bedroom as the risk of falling out of bed is often high to monitor the individual's movements and surroundings. However, few places are as sensitive to a person's privacy as the bedroom; effectively, installation should take place depending on the purposes and functions of the technology to ensure all content within the sensor's range is limited. The sensor range is limited to a maximum distance and sensitive to certain materials and sunlight, reducing the sensor's function. The field is also affected by the light reflectivity of materials that the IR light hits. This means that materials, such as dark denim and leather, with low light reflection, will reduce range. Mirrors, glass surfaces and giant screens can also give erroneous light reflections that give RoomMate a distorted image of the room and reduced function. If a person moves very close to the sensor, much of the emitted light will be reflected, and the sensor may be temporarily blinded and have reduced function.

2.2.2 Invasive technology

An alarm system can be interpreted as a technical facility for notifying alarm recipients or personnel, via an alert signal, that the situation in the patient's room has changed and of critical events that may require physical assistance. [45] When used to provide healthcare with vulnerable patients with limited capability to give valid consent, intrusive measures such as 'invasive warning systems' [46] may legally be recognised as use of force. [47] The municipality may

---

[42] RNJ, "Roommate, Installasjonsveiledning, Rev D." 4.

[43] Ibid, 3.

[44] RoomMate.no, "Roommate Ofte Stilte Spørsmål – Faq," https://www.roommate.no/faq/.

[45] Prop. 90 L (2012-2013) Endringer i pasient- og brukerrettighetsloven mv. (bruk av varslings- og lokaliseringsteknologi)" [Changes in the Patient and User Rights Act (use of alarm and location technology - Proposition on legislation to the Storting], pt. 3.1.

[46] HCSA, Section 9.

[47] HCSA, Section 9-2 para. 2.

implement 'notification and location technology' upon a risk and proportionality assessment [48] thus, whether the RoomMate technology is invasive needs assessing its scope for application.

Invasive technology is defined by the Norwegian Health Directorate as:

> 'all tracking, locating, monitoring and sensor technology that sends information to third parties about the patient or user's situation, action, movements without the patient or user initiating it' *(author's translation)*. [49]

Examples of invasive technology are technologies that alert others when the patient does or does not do anything, e.g., moves in and out of bed, falls, does not take medication or open the refrigerator etc. Technologies that track or localise individuals and transmit this information to other persons and technologies meant for surveillance of individuals using audio and image for shorter or longer periods. [50] Seeing as the RoomMate technology can fall within the category of invasive technology, one or more legal grounds to utilise the invasive technology and lawfully process personal and health data is required.

2.3 Privacy and security of personal data and ICT systems: Establishing roles and requirements

Many actors and information in processing health data are often shared across central and local healthcare providers, response centres, suppliers of equipment or other services, and sub-suppliers. Today's technological landscape is mainly self-regulated by contracts, standard contractual clauses, and conditions issued by the government or the EU. As RoomMate process health data on behalf of the municipality, RoomMate and its employees may be exposed to confidential information by delivering a service following a purchase agreement. The overall responsibility lies with the municipality as they must ensure that the supplier with whom it enters into a contract can fulfil requirements for requested services.

---

[48] PURA, Section 4-6 a.

[49] Kommunesektorens Organisasjon (KS), "Velferdsteknologiens Abc," [The ABC of welfare technology.] (2016).

[50] Kommunesektorens Organisasjon (The Norwegian Association of Local and Regional Authorities) «Velferdsteknologiens ABC», 9.

Often, a supplier of ICT offers much functionality and possibilities than the municipality may legitimately accept. [51] Therefore, the municipality cannot settle for a fixed package deal provided by the supplier, and there is a need for proper and close management control. As part of the public tender of welfare technology, Oslo's local health agency specified 117 requirements as part of the tender calls. Eighty-three of these were minimum requirements that the supplier must comply with, and 34 were evaluation requirements where interdisciplinary teams gave points to assess the conditions. If minimum requirements were not satisfied as part of the tender calls, the purchase and legal team would evaluate the service offer. [52]

2.3.1 Relevant sources

Personal data [53] has been defined expansively by its legal definition [54] and case law [55] to protect the fundamental rights of data subjects. [56] This engages a lot of information about data subjects and a strict liability regime caught by various organisations irrespective of sector. [57] Moreover, the material scope of the GDPR is defined in a broad sense to apply to any processing, either manually or automatically, of personal data that form part of a filing system. The mere possibility of identification will render data 'personal' under the GDPR. [58]

European privacy and data protection law clarifies the duties of data controllers and processors on one side and the rights of natural persons and data subjects on the other. It sets out a strict liability scheme with notification requirements and sanctions enforced by the national DPA to regulate reactively. Also, the GDPR sets out operative provisions with a forward-looking approach for safeguarding the privacy and information security. The most innovative attempt to protect these interests is reflected in Article 25. This provision obliges the controller to implement appropriate technical and organisational measures designed to implement data protection principles. While the processor may initiate such actions, no independent duty

---

[51] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.

[52] Ibid.

[53] See Chapter 1, Section 7.2.

[54] Article 29 Data Protection Working Party (WP29), "Opinion 4/2007 on the Concept of Personal Data, 20 June 2007 (‘Wp 136’)."

[55] Case C-101/01 *Bodil Lindqvist.*

[56] Ibid.

[57] GDPR, Article 4 (1).

[58] Paul Voigt and Axel von dem Bussche, *The Eu General Data Protection Regulation (Gdpr): A Practical Guide* (Cham: Cham: Springer International Publishing AG, 2017).

exists upon them for assessment. Tendencies of outsourcing or purchasing ICT services from private organisations suggest that data controllers in the municipality's healthcare agency are often not engaged in the development and design stage. The obligations do not directly cover suppliers. [59] This distribution of responsibility might predict that suppliers cannot deliver their services since the controller cannot comply with the legal requirements. [60]

Following the requirements in the tender calls, RoomMate must comply with the regulatory requirements to privacy data protection and information security and the requirements for the Code of Conduct for information security and privacy in health and care services (Normen). [61] The non-exhaustive list includes the Personal Data Act, GDPR, the Health Records Act, Personal Health Data Filing System Act [62], Health and Care Services Act (HCSA), Health Personnel Act and the Patient and User Rights Act (PURA). [63] Standards, examples, and information material issued by governmental and guiding actors should be used by the municipality to share common knowledge and handling with digital transformation processes. [64] The Code of Conduct for information security and data protection in the healthcare and care service (Normen) issued by the Norwegian Directorate for e-health [65] is an agreed set of requirements for information security and data protection used across the healthcare sector. [66] Therefore, it offers an interpretation of the legislation and cannot be considered the primary reference source as this is not binding legislation. Examining the legal basis for specific requirements in Normen is subject to critical review for mapping against the statutory authority to evaluate the coherence and consistency of its interpretation. [67] Only organisations that commit

---

[59] Åste Marie Bergseng Skullerud, "Personvernforordningen. Lovkommentar, Artikkel 25. Innebygd Personvern Og Personvern Som Standardinnstilling, Juridika."

[60] Ibid.

[61] Norwegian Government's Standard Terms and Conditions for IT Procurement (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision " (2018).

[62] Lov 20.juni 2014 nr. 43. Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) [Personal Health Data Filing System Act].

[63] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[64] Such as Norwegian Digitalisation Agency (Digdir), "Internkontroll I Praksis - Informasjonssikkerhet [Information Security Management System in Practice] (Version 1.5) " (https://internkontroll-infosikkerhet.difi.no/).

[65] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen) [Code of conduct for information security in the health and care sector]. "Faktaark 10 – "Bruk av databehandler (ekstern driftsenhet), 4."

[66] ISO, "Iso 27001:2013 Information Security Management System - Isms," (2013).

[67] Henrik and Teie Hellum Ulseth, Petter., "Vurdering Av Helseetatens Etterlevelse Av Normens Krav Til Konfidensialitet Og Tilgangsstyring" (Master thesis, University of Oslo, 2020).

are obliged to follow requirements in Normen; this includes Oslo municipality and RoomMate. [68]

2.3.2 The role of the municipal healthcare service

The purpose of HCSA is to set out the municipality's overall responsibilities and obligation [69] and ensure due process protections for the rule of law and limit abuse of power and compulsion to patients with mental disabilities. [70] The municipality must provide necessary healthcare services to citizens [71] and ensure professional conduct, patient safety and quality. [72] This shall include all patient and health care user groups [73] who receive healthcare services at home, institutions, and nursing homes. [74] Notably, the municipality has to ensure that healthcare services are conducted responsibly. [75] Thus, the patient shall receive a comprehensive, coordinated, and worthy healthcare offer. Also, the municipality must ensure that personnel who provide the services can comply with statutory duties, [76] e.g. the Health Personnel Act's duty of confidentiality, documentation, and information [77] and exemptions and prohibitions that follow.

2.3.2.1 Data processing agreement

Whether RoomMate acts as a joint controller or processor is crucial in clarifying duties and obligations and whether a data processing agreement is needed. Two or more controllers jointly decide the purposes and means of processing; these shall be joint controllers. [78] The factual basis is that when signing the contract, a data processor agreement was entered into [79] by Oslo municipality and HEPRO, a distributor of the RoomMate as a supplier of IT software and equipment to the municipality. [80] The agreement stipulates that RoomMate is the

---

[68] RNJ, "Roommate, Oversikt Personvern Og Datasikkerhet, Rev A," ed. RoomMate AS (Roommate.no2020).
[69] HCSA, Chapter 1 Section 1-1.
[70] Ibid, Chapter 9.
[71] Ibid, Section 3-1, para. 1.
[72] Ibid, Chapter 4.
[73] Ibid, Section 3-1, para. 2.
[74] Ibid, Section 3-2 (6) lit. a-c.
[75] Ibid, Section 4-1.
[76] Ibid, Section 4-1.
[77] Health Personnel Act, Chapter 6.
[78] GDPR, Article 26 (1).
[79] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".
[80] Interview with Oslo municipality, 26 April 2021.

processor on behalf of the municipality. [81] RoomMate shall thus only process personal data on behalf of the municipality and cannot decide the purposes and means of processing. What role HEPRO plays as the distributor is highly relevant; however, it is outside the scope of this paper and will not be addressed further as the focus is the roles and responsibilities of the municipality and RoomMate AS as an ICT supplier.

CJEU case law has interpreted controller under Article 4(7) in a broad sense. The municipality is the data controller for processing personal health data by implementing ICT service from RoomMate as a supplier. The controller is the responsible party that decides the purposes and means of processing personal health data.[82] Seeing as the municipality has specific regulated obligations and commitments to provide justified services to citizens, they must be the controller of data to decide the purposes and means, i.e., why and how particular personal health data is collected and processed. The essence of the agreement should be communicated to the data subject, [83] yet RoomMate does not have any independent responsibility to fulfil similar legal obligations. Therefore, the municipality must set requirements for the supplier regarding compliance with regulations in specific minimum and evaluative requirements in the public tender and subsequent agreement after the tender is won.

2.3.2.2 Controller responsibility

The municipality will always be responsible, i.e., controller for processing health and personal data connected with public healthcare services. [84] The municipality must follow up the data processing agreement, as the implementation of the RoomMate technology involves the processing of personal health data. [85] This also requires that the designated data protection officer (DPO) in the public body advise how the organisation should demonstrate compliance. [86] The agreement shall also state the extent to which processing shall occur and the duration, which is decided based on processing. [87] Also, the municipality completed several requirements to

[81] Ibid.

[82] Case C-131/12 *Google v Spain.*

[83] GDPR, Article 26 (2).

[84] Normen, "Faktaark 46 - Personvern Og Informasjonssikkerhet Ved Tjenesteutsetting Av Kommunale Helse- Og Omsorgstjenester_5.0.Pdf."

[85] GDPR, Article 35 (1).

[86] GDPR, Article 37 (1)(a).

[87] GDPR, Article 28 (3), para. 1.

quality-check security requirements as part of a comprehensive acceptance test and security audit of RoomMate before implementation. [88]

2.3.2.3 Processor

RoomMate is obliged to process all information following the agreement and comply with the controller's security requirements. Also, they are compelled to commit to the confidentiality of the personal data they are processing and follow the controller's acceptance criteria and [89] document results from completed risk assessments, also from sub-suppliers. If the controller's security audits of the data processor show that this is necessary, the processor should have the possibility to make changes to the agreement. This means that RoomMate cannot enter into agreements with sub-suppliers unless this is agreed in writing with the municipality beforehand. [90] For example, a minimum requirement is that the supplier performs continuous penetration tests to check their solution and system. [91] As this engages a sub-supplier, [92] it is necessary to agree on this beforehand.

2.3.3 Risks to information security

Protection of personal data and information security (IS) are fundamentally linked to each other. All documents, journals and registers of an administrative agency are defined as public, except as otherwise provided by statute or pursuant regulations. [93] Any person may apply to an administrative agency to access case documents, journals and registers of that administrative agency. The purpose of these requirements is to facilitate public entities operating in open and transparent management and facilitate the re-use of public information, which is essential for democratic and societal interests. The need for confidentiality in the public sector must therefore be anchored in a statutory provision. The most common exemption provisions are set out in the Public Administration Act, Section 13 (duty of confidentiality) [94]and Chapter 3,

---

[88] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[89] GDPR, Article 28 (3).

[90] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[91] Ibid. pt. 6.38.

[92] Interview with employee in RoomMate AS. 15 March 2021.

[93] Lov 19.mai 2006 nr.16. Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova). [Act relating to the right of access to documents held by public authorities and public undertakings - Freedom of Information Act], Section 3.

[94] Lov 10.februar 1967 nr. 00. Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) [Act relating to procedure in cases concerning the public administration - Public Administration Act].

which includes exceptions from the right of access. The purpose of ensuring IS is to support primary objectives and is not a primary aim on its own. [95] In this context, the primary aim of the municipality is to maintain the core activities of the healthcare service. With this, the most essential is the provision of basic services. Thus, it is imperative to keep data confidential, given that it is often sensitive information. Still, equally important is the availability of ICT systems and components to provide essential functions of the care services. The main risks pointed out by RoomMate is the potential for threat actors to hack or otherwise gain unauthorized access to their systems. This can have damaging and even lead to life-threatening consequences for patients, staff, and the municipality's reputation controlling and processing sensitive personal data. Strategies for risk management involves the option to either accept, avoid, mitigate, or transfer/share the risk in question. For example, the municipality may not have the means necessary to provide essential healthcare services if it spends an overwhelming amount of cybersecurity measures. On the other hand, this factor should be balanced with the threat scenarios most likely. Perhaps the risk of a cybersecurity threat could be mitigated by implementing other organizational measures and a robust security management system.

The municipality is responsible for ensuring that information security and privacy requirements are complied with throughout the supply chain by implementing measures ensuring that processing is performed lawfully, transparently, and fairly [96], review and update such steps [97] to set requirements for built-in security. [98] The controller is obligated to determine the level of protection based on the relevant risks for processing personal data in question [99] and ensure an overview of processing health data with a management system for information security (ISMS). Necessary technical measures relate to logging, access control, central server solution, storage, and data sharing. According to RoomMate's Privacy Policy, there is no permanent audio, images, or video storage. [100] Also, the central server solution is physical servers located in a data centre in Norway; only authorized employees are given access. [101]

---

[95] *Høringssvar - Nou 2018: 14 Ikt-Sikkerhet I Alle Ledd Og Utkast Til Lov Som Gjennomfører Nis-Direktivet I Norsk Rett*
, 21.03 2019., 2.

[96] GDPR, Article 5 (1)(a).

[97] Ibid, Article 24.

[98] NOU 2018:14 «IKT-Sikkerhet i alle ledd» [ICT Security at all stages], 11.

[99] GDPR, Article 32.

[100] RoomMate.no, "Roommate as Personvern Policy," https://www.roommate.no/personvernpolicy/.

[101] RNJ, "Roommate, Oversikt Personvern Og Datasikkerhet, Rev A.", 2.

2.3.3.1 Acceptance and security tests

The local healthcare agency in Oslo municipality can make procurements that become group-wide. [102] Suppose a borough opts for the purchase of RoomMate. In that case, this can be carried out without a complete procurement procedure as the municipal authority does this as quality assurance of the supplier. [103] This involves conducting risk assessments and security review on behalf of all the boroughs within the municipality. [104] As it may be challenging to follow up with each borough, the municipality has a specific managerial responsibility to follow such procedures. The acceptance test of RoomMate took around six months, where a review of the security of RoomMate, risk and vulnerabilities (ROS) analysis and DPIA was part of this to follow up and verify that RoomMate responded to all the requirements in the final competition. The supplier was also required to perform a DPIA and obliged to commit to the confidentiality of the personal data they are processing and follow the controller's acceptance criteria. [105] If the municipality's security audits of RoomMate show it is necessary, changes to the data processing agreement can be made by the processor.

2.3.3.2 Risk assessment (DPIA)

Before processing, the municipality and RoomMate were obligated to perform a DPIA. As Article 35 is limited to high-risk situations and requires documentation of measures to evidence the organizations' compliance, [106] RoomMate must document completed risk assessments and penetrations tests conducted by them and sub-suppliers. [107] Any risk concerns possible consequences and associated probabilities for events to occur or choices that are done to present a combination of the size of one risk. [108] Innovative technology that involves systematic monitoring in the implementation of digital supervision and sensor technology, by which information is potentially processed at a large scale, requires knowledge of risks, especially seeing RoomMate is used to assist vulnerable patient groups. Identifying the consequences of

[102] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.
[103] Ibid.
[104] Ibid.
[105] GDPR, Article 28 (3).
[106] GDPR, Article 35 (3)((a)-(c)).
[107] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".
[108] Norwegian Digitalisation Agency (Digdir), "Internkontroll I Praksis – Informasjonssikkerhet. Grunnleggende Begreper [Information Security Management Systems in Practice. Basic Concepts].", 3-4.

various relevant scenarios and assessing how likely a breach is to occur is part of such assessment. The municipal management that decides the risk appetite work as guidelines to implement appropriate measures so that the use of RoomMate does not surpass the tolerance level. [109] Risk exposure is about the activity level of the individual. [110] The risk of falling can have many severe outcomes, both mentally and physically, not only for the patient but also their next of kin, families and neighbours who fear that the risk of injury is high. The risk-based assessment in GDPR deals with risks for all those involved: data subjects, controllers/processors, and third parties. This means that many factors from different perspectives are to be assessed before given a justified level of priority and involves setting any grounds the controller might have *not* to implement a potential measure. The municipality required that it should not be possible to enter the system and obtain information arbitrarily. While main risks were addressed and assessed, some risks have not been completely reduced. For example, there is a risk of using smartphones to conduct supervision, which can easily be accessed and utilised amongst other persons. Suppose others can see the visual images of the patient or the user is unaware that medical records are kept and can be accessed via the phone. In that case, this could lead to more severe risks to the security and protection of sensitive information about patients.

2.3.3.3 Local storage and sharing of data

Suppose sensitive data, such as detailed images and sound, is stored. In that case, this can have significant negative impacts on the rights and freedoms of elderly patients with mental disabilities or otherwise reduced cognitive functions if unauthorised access is given. In general, the purpose limitation principle prohibits the processing of personal data for a purpose besides the original purpose, [111] with exceptions for scientific and historical research objectives, statistical and archival goals in the public interest. [112] The purpose also determines the storage time as personal data shall not be stored longer than is necessary for the original purpose. [113] HCSA Section 5-10 sets out an obligation on the municipality and 'activities that

[109] Datatilsynet (DPA), "Software Development with Data Protection by Design and by Default," (2017).

[110] D. A. Skelton et al., "Prevention of Falls Network Europe: A Thematic Network Aimed at Introducing Good Practice in Effective Falls Prevention across Europe," *European journal of ageing* 1, no. 1 (2004).

[111] GDPR, Article 5 (1)(b).

[112] GDPR, Article 5 (1)(b).

[113] GDPR, Article 5 (1)(e).

have an agreement with the municipality to provide healthcare services [114] to ensure that the electronic health record (EHR) and information systems for the activities are adequate. This means that effective electronic coordination and further development of records and procedures must be considered in procurement. [115] This implies that RoomMate must ensure a level of protection and effectiveness of medical record-keeping and procedures. A minimum requirement was that the RoomMate system could be integrated with the National Welfare Technology Hub (VKP) [116] , which unlocks the potential to conduct record-keeping directly in the EHR. In Oslo municipality, RoomMate ewill be used conjointly with VKP. [117] VKP is a service from the Directorate of e-Health, a sub-ordinate institution of the Norwegian Ministry of Health and Care Services, that handles data flow between welfare technology solutions and other e-health systems, such as EHR. [118] As the RoomMate technology will transmit information automatically to EHR, the solutions must be able to configure in a way that only relevant and necessary communication is sent over. [119] The use of VKP to perform direct record-keeping in EHR required integration of the technology and the electronic record system, and the testing this considerable time. [120] This may be a more effective way of documenting health records. It means the healthcare provider does not need to spend unnecessary time and effort managing multiple technical devices and could mean more accurate information is recorded. For example, using various dissimilar systems and devices could be time-consuming and direct record-keeping could save resources and provide more precise information. Still, this means that a lot of sensitive information will be transmitted via the RoomMate application, and this must be managed and controlled to ensure the values of the CIA. Storing and sharing shall also follow the general rules for processing personal data as it must show a specified purpose and legal basis for processing. If sound and image are used as part of a filing system established for therapeutic purposes, then storage should occur regularly. [121] The municipality

---

[114] HCSA, Section 5-10.

[115] HCSA, Section 5-10.

[116] In Norwegian, 'Velferdsteknologisk knutepunkt' (VKP).

[117] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.

[118] "Velferdsteknologisk Knutepunkt (Vkp)," Direktoratet for e-helse, https://ehelse.no/velferdsteknologi/velferdsteknologisk-knutepunkt-vkp.

[119] Normen, "Veileder Informasjonssikkerhet Og Personvern Ved Bruk Av Velferdsteknologi 3.0.."

[120] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.

[121] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), "Veileder for Bruk Av Video, Lyd Og Bilde I Helse-Og Omsorgssektoren Versjon 2.0," (Direktoratet for e-helse, Helse- og omsorgsdepartementet, 2021).

must draw a clear line to distinguish between real-time information and what data is stored so that sensitive information such as video, sound and audio is stored locally.

2.3.3.4 Access control and logging

Following the risk assessment, the municipality is obligated to ensure logging. Many requirements were set in the tender calls, so RoomMate also has responsibilities to ensure ac to health information is controlled by appropriate measures. Not keeping a log of activities by the system's users can have severe effects as users could gain access to the system and information about patient's medical records either intentionally or unintentionally. ECHR jurisprudence [122] holds that it is ultimately the positive obligations of state governments to ensure logging is required by law to authenticate user access. RoomMate must have adequate password protection, two-factor authentication, and a set timer to a maximum of sixty seconds for each performed supervision. [123] This is a way to avoid unlimited access and a default security mechanism that protects access controls by default.

The administration system of RoomMate receives alerts from all deployed sensor units, and such warnings must be logged. [124] A description of the various types of alerts that are logged and how this is done is also required. The municipality's management must ensure that any deviations are logged and controlled. [125] At a bare minimum, specific activities must be logged [126] , such as the unique identifier for the authorized user, the type of information given access to, any changes of data, users having access to health information relating to the patient's name and or birth/identification number, the reason for access as well as the time, date and duration of access. [127] Further, logs of safety significance must be kept, including registration of authorized use and attempts at unauthorized use shall be retained until no longer of use in the healthcare service.[128] Further, any registration, change, correction and deletion of medical records is required. [129] These requirements are essential measures to safeguard the

[122] Application no. 20511/03 Judgement of 17 July 2008 *(I v. Finland*).
[123] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.
[124] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".
[125] Normen, "Veileder Informasjonssikkerhet Og Personvern Ved Bruk Av Velferdsteknologi 3.0.."
[126] Normen, Chapter 5.5.4.
[127] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".
[128] Normen, Chapter 3 (confidentiality).
[129] Normen, Chapter 3 (integrity).

CIA of information and systems and avoid unauthorized or unnecessary access to detect a potential personal data breach.

2.3.4 Encryption

All communication outside of the municipality's control must be encrypted. [130] All encryption and decryption between communication points in the infrastructure must be done using approved equipment that the organisation controls. In the case that RoomMate as a supplier is used for this, it must be ensured that the data processing agreement covers their processing of personal data. [131] As a minimum requirement and to limit the access by specific roles, such as system administrators, stored information must be encrypted. [132] Also, any communication over the Internet, in databases and on mobile units, encryption is needed for all parts of the value chain. [133] When supervision is carried out or when an alarm or notification is to be sent, this information is sent to the RoomMate.no server. [134] The sensors communicate via an encrypted VPN channel with a physical server («RoomMate.no») owned by RoomMate AS and located in a data centre in Oslo. Encryption is considered personal data and must be processed according to related principles. [135] The objective of encryption is to protect the confidentiality of information in a communication channel between two identified parties.[136] Advanced encryption can protect confidential information by rendering the data unintelligible to unauthorized actors without the needed key for decrypting the message. This does not necessarily mean the confidential information is anonymous because if the key is available, there is a possibility to identify the data subject.[137]

---

[130] Normen, Chapter. 5.3.5

[131] Ibid.

[132] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[133] Ibid. pt.6.36.

[134] RNJ, "Roommate, Systemarkitektur, Rev E," (roommate.no: RoomMate AS, 2021).

[135] Datatilsynet (DPA), "Anonymisering Av Personopplysninger. Veileder," (2015)., 10.

[136] Ibid.

[137] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

3 Legal analysis

Oslo municipality's responsibility as a controller is to assess the legal justification for processing personal data about patients and employees. The legal basis must cover all health and personal data processing types, including data collection, data storage, deletion, and disclosure. [138] In the healthcare sector, there are many obligations and exemptions for processing health information. A need to retrieve data for the benefit and interest of patient's safety and welfare could be legitimate, yet whether and what type and the amount of data involved and the specific purpose is for processing are vital factors for the municipality to evaluate. The use of welfare technology generates a lot of information about patients. Whether the collection and storage of the data are relevant and necessary to provide services must be evaluated. By adopting RoomMate as part of their healthcare service provision, the municipality is responsible for safeguarding the professional duties of documentation and confidentiality of healthcare personnel and the patient's right to safe healthcare services and privacy.

3.1 Personal data and data concerning health

Upon registering the worker and patient, information as personal data and special categories must be filled in by the system administrator. The system stores login information, telephone number, name, last name, birth number and potentially other types of information from individuals with login access, i.e., the health personnel and other system users. Further, RoomMate stores information that, in some instances, can identify the patient. [139] This includes the first and last name, birth number and address or residence unit of the patient. [140]

3.1.1 Data types and special categories

Name, identification number are specific examples of identifiers mentioned in the definition of personal data in the GDPR. [141] Other identifiers specific to 'the physical, physiological, genetic, mental, economic, cultural or social identity' of the patient and health personnel could be processed. Video, image and sound components are also involved, which strongly suggests

[138] "Norm for Informasjonssikkerhet Og Personvern I Helse Og Omsorgstjenesten (Normen) ", ed. Helse- og omsorgsdepartementet Direktoratet for e-helse (normen.no 2020).

[139] RoomMate.no, "Roommate as Personvern Policy".

[140] "Roommate Nyheter Og Referanser," https://www.roommate.no/referanser/.

[141] GDPR, Article 4 (1).

that data sensitivity is high as physical and physiological factors such as the patient's body shape, and behavioural patterns are vulnerable for continuous, close monitoring. Further, the intended implementation of increased collaboration across municipal and regional health institutions to gather information in one joint electronic health record [142] could suggest that processing and storage of personal data will become more centralised, and vulnerabilities could increase. As numerous types of personal data and identifiers have pointed out, personal data is involved.

3.1.2 Risks of anonymisation

As anonymous information falls outside the GDPR's liability regime scope, [143] actors, including the municipality and RoomMate, have a solid incentive to anonymise data. Images and audio should always be used in anonymous form [144] to protect the privacy of data subjects. Healthcare providers can then use important data for medical research, statistical or training purposes without jeopardising the duty of confidentiality. [145] Techniques for achieving this could mean that faces are skidded and voices distorted.

Anonymous information can be interpreted as the opposite of personal data, namely any information *not* related to an identified or identifiable natural person. Anonymisation aims to prevent individuals from being recognised in a data set by manipulating information,[146] using techniques to conceal or delete information. [147] A method is to avoid a set of attributes of personal information being paired. [148] Risks to the potential to single out, link records and derive information concerning an individual. [149] Suppose data such as the image and sound of the patient can be anonymised, and the individual is no longer identifiable. In this case, information

---

[142] Meld. St. 9 (2012–2013) "En innbygger – en journal" [One citizen – one health record].

[143] GDPR, Recital 26.

[144] (Normen), "Veileder for Bruk Av Video, Lyd Og Bilde I Helse-Og Omsorgssektoren Versjon 2.0."

[145] Lov 2. juli 1999 nr. 64. Lov om helsepersonell m.v. (helsepersonellloven) [the Health Personnel Act], Section 23.

[146] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA law review* 57, no. 6 (2010).

[147] Samson Esayas, "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing' Approach," *European Journal of Law and Technology* Vol 6, No 2. (2015).

[148] (DPA), "Anonymisering Av Personopplysninger. Veileder."

[149] Article 29 Data Protection Working Party (WP29), "Opinion 05/2014 on Anonymisation Techniques " (2014).

ceases to be 'personal data' and data protection principles will not apply. [150] All means' reasonably likely' to link information back to an individual ought to be considered. [151] This involves assessing how probable and difficult it is to identify the patient. Objective factors related to times, costs, and technology available on the market should be evaluated to define how likely it is for someone possibly identifying the patient. That a person is identified means that someone can be singled out from a group of people; thus, a direct identification of a patient as seen by the infrared image is likely not possible. Yet, this is not all required for data to be rendered anonymous as the inclusion of 'identifiable' indicates that a mere possibility of identification is, per definition, personal data. That identification is possible in the future [152] or by linking other types of information [153] are sufficient grounds to satisfy the aspect of '*identifiability'*.

3.1.2.1 RoomMate's technique

A minimum requirement was a remote supervision solution with anonymised and detailed image/video. [154] As their technique, RoomMate allows 'anonymous supervision' achieved by infrared images visualising the physical silhouettes of the individuals to see where they are in the room (e.g., sitting [155] or lying on the floor [156]). Audio communication is anonymised by distorting the sound in the room. RoomMate also offers a range of physical alarm units in the shape of alarm watches, neckless, panic button, pull cord and a wireless door sensor [157] as options that can be integrated with or without the instalment of the sensor. Thus, it can handle a range of active sensors that will send out relevant alarms or alerts if the patient activates it or enters the room. In cases where multiple sensors work together, they can generate comprehensive information of an individual's movement patterns and similar information corresponding

[150] Esayas, "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing' Approach."

[151] (DPA), "Anonymisering Av Personopplysninger. Veileder.", 14.

[152] (WP29), "Opinion 05/2014 on Anonymisation Techniques ".

[153] Esayas, "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing' Approach.".

[154] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[155] See *fig.2.4.*

[156] See *fig.2.5.*

[157] RoomMate.no, "Roommate Anonymisert Tilsyn Og Pasientvarsling".

to information collected by a traditional video camera or microphone. [158] This raises further questions about whether the info is effectively anonymised or not.

3.1.3 Is data processed by RoomMate anonymous?

When assessing the effectiveness of anonymisation, an examination of the objective of the processing is needed. [159] If the underlying goal of processing patient information is to identify them, it may be challenging to achieve adequate anonymisation. [160] RoomMate's technique aims to avoid identification by relying on images from the sensor as 'anonymous' images. Still, that an individual is not visible from pictures or that content of speech can be accessed does not necessarily mean that the data collected is anonymised. The fact that the sensor detects real-time status and events relating to the patient suggests that information *about* the event, such as a fall and potentially *where* this happened, might be crucial for providing necessary care. Assuming that the objective of implementing RoomMate technology is to help patients if they suffer from a fall or injury, one could argue that the processing necessarily involves a need to identify the individual. [161] Even if it is impossible to determine the patient through infrared images and distorted sound, this does not render information effectively anonymous. Suppose a health worker has knowledge of patient information and that the patient lives alone. The fact that the worker can see or is alerted via RoomMate that this patient has fallen and can resonate with potential causes that have led to the fall could still be considered processing of personal data.

3.1.3.1 Value of anonymised data

The total gross domestic product of the EU's digital economy will nearly double by 2025, emphasising the great value of data. [162] This means data that requires protection must be shielded but also made visible when permissible. The potential to use health data for research or medical analytical purposes could be valuable and openly shared if it can be genuinely anonymised. Collecting information with image and audio content is likely not publicly disclosed as

---

[158] Ida Victoria Rullestad Odland, "Hjemmelen for Å Bruke Varslings- Og Lokaliseringsteknologi Som Helsehjelp Til Mennesker Med En Demensdiagnose. En Drøfting Av Reguleringene I Pasient- Og Brukerrettighetsloven Kapittel 4a Og § 4-6 A." (Master thesis, University of Bergen, 2018).

[159] Esayas, "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing' Approach.", 9.

[160] (WP29), "Opinion 05/2014 on Anonymisation Techniques".

[161] See *fig.2.4.*

[162] In 2018, data economy was 2,4 % of EU's GNP. In 2025, this is to rise to 5,8 %.

only accessible for authorised users upon professional secrecy to keep patient information strictly confidential. All detection of events is processed locally by the RoomMate sensor [163] , implying that sensitive data is only sent out from the sensor in an alarm situation or when users with access carry out supervisions. Even though anonymising images and the sound of patients usually preclude the applicability of the GDPR, there are other data processed by RoomMate that all together argue for the need to safeguard individuals' rights and freedoms. In this context, data subjects form a particularly exposed group with limitations due to age, mental or cognitive capacity. To what extent the information gathered is anonymous will depend mainly on the specific context and what types of data are processed. If both image and sound are genuinely anonymised, it should likely not be possible to re-identify any information relating to an individual. If information is linked to an individual, and the individual is identifiable, then this must be considered personal instead of anonymous data. Legal [164] and technical [165] scholars agree that, at the current rate of advancements of anonymisation techniques, the legal distinction between identifiable and non-identifiable information is not sustainable. [166] The WP29 reinforces this view as that data can only be genuinely anonymous when anonymisation is irreversible, i.e., impossible to reverse-engineer. [167] This sets a threshold impossible to manageably comply with or enforce given the increased likelihood for re-identification of individuals from anonymised data sets. This argues that anonymisation must be a permanent action that is worthy of solid protection as any possibility of identification will render data subjects effectively identified or identifiable.

3.1.4 Data concerning health

It can be assumed that data concerning health is involved as processing information is collected to provide health care services. As one of the special categories of personal data caught by GDPR, Article 9(1) constitutes a particular sensitive category of personal data worthy of strengthened protection. [168] Its legal definition has awarded the scope for application an expansive is:

---

[163] Interview with employee in RoomMate AS. 15 March 2021.

[164] Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.", 1776-1777.

[165] A. Narayanan and E. Felten, "No Silver Bullet: De-Identification Still Doesn't Work" (2014).

[166] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of Eu Data Protection Law," *Law, Innovation and Technology* 10, no. 1 (2018).

[167] (WP29), "Opinion 05/2014 on Anonymisation Techniques ".

[168] GDPR, Recital 53.

'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the individual's health status.' [169]

CJEU jurisprudence has also interpreted this category of personal data in a broad sense to engage all aspects of an individual's mental and physical health state, [170] including any information connected to the data's current, past, and present health condition subject. [171] The definition includes at least information as defined in national health legislation, including confidential information according to the Health Personnel Act Section 21 [172] and other information and assessments that can be linked to an individual, revealing information about or of significance for health, for example, the Health Records Act. [173]

To 'reveal' health information, a link between the information processed and the individual's health status can be construed in a broad sense to engage all data about an individual's health, both directly and indirectly. [174] This also includes this situation where several data types can lead to revealing health information about the patient. While records of medications indeed show information about health status, continuous observation and logging of behaviour and alerts may reveal similar information types. For example, the ID number for secure identification and recovery in a healthcare context is considered health data. [175] Moreover, information about family members can also be regarded as health data because information such as hereditary diseases come into play. [176]

It is prohibited to process data of this category unless the processing is necessary under at least one of the alternative conditions in Article 6(1). This category also requires a

---

[169] GDPR, Article 4 (15).

[170] GDPR, Recital 35.

[171] Case C-101/01 *Bodil Lindqvist.*

[172] Åste Marie Bergseng Skullerud, "Personvernforordningen. Lovkommentar, Artikkel 4. Definisjoner, Juridika ".

[173] Lov 20. juni 2014 nr. 42. Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) [the Health Records Act], Section 2.

[174] See Chapter 1, Section 7.2.

[175] Skullerud, "Personvernforordningen. Lovkommentar, Artikkel 4. Definisjoner, Juridika ".

[176] Ibid.

supplementary legal basis and the fulfilment of at least one alternative condition in Article 9(2). [177] Nevertheless, the inclusion of Article 9(4) provides member states considerable room for discretion to shape national rules on processing this category. [178] Recital 53 particularly mentions a legitimate need to process such data for 'health security' and 'monitoring and alert' purposes. Also, Member States can implement further conditions and limitations on processing such data unless it hinders cross-border data flow on the single digital market.

Undoubtedly, information about an individual in a healthcare context can be applied to this case study. Showing physical, behavioural patterns of vulnerable patients falls within this category. Also, processing various types of special categories altogether implies a necessity for applying data protection principles. Moreover, the threshold for labelling information as data concerning health is relatively low, seeing as the scope of personal data is extremely broad. For the reasons mentioned, it is a valid assumption to state that data concerning health applies.

3.2 Lawfulness of processing

3.2.1 Principles of purpose limitation and specification

It is prohibited to process personal data without a specific purpose. [179] Even if a justified goal of processing personal data is established, other grounds are required for processing to be lawful. The principle of purpose limitation requires a legitimate, justified purpose explicitly specified to ensure legal processing. [180] In the given context, a purpose of processing health data is to detect health damage at an early stage, prevent or reduce risks of such damage from occurring, and safeguard the patient's privacy. [181]

Four main functionalities requested by the municipality was to notify when a patient moves in and out of bed, in and out of the room, they fall or lie down within a given area, as well as a visual supervision function that does not necessitate physical presence. [182] The purpose of the

[177] Kuner Christopher et al., *The Eu General Data Protection Regulation (Gdpr) : A Commentary* ([Place of publication not identified]: OUP Oxford, 2018), Book.

[178] Bygrave, Lee Andrew & Tosoni, Luca (2020). Article 4(15): Data concerning health in ibid.

[179] GDPR, Article 5.

[180] Ibid, Article 5 (1)(b).

[181] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[182] Ibid, Main functions A-D, 7-10.

alert functions is to prevent or detect risks of health damage to the patient. [183] The purpose of visual supervision is to safeguard the privacy and undisturbed sleep of the recipient. [184] These purposes suggest that the purpose limitation principle is satisfied as the aim is in the interest of the patient's safety, privacy, and well-being. Still, a purpose for processing must be explicit, not ambiguous. The need, measures, and examples of how the intended purpose may be achieved are specified further. These mainly stem from a need to prevent and detect high-risk situations early and automatically alert health personnel as quickly as possible. [185]

Another purpose could stem from the municipality's legal obligation to offer necessary healthcare services.[186] Most often, citizens have trust in the legitimacy of the healthcare service. There will always exist risks for breach of duties and abuse of patients and health information. However, strict requirements are set for health personnel and their responsibility of professional conduct. Moreover, there are general obligations upon the municipality in the HCSA's objective clause to *prevent, treat and facilitate* to cope with diseases, injury suffering and disabilities' [187] to patients. Concerning dignity and integrity [188], the patient shall be offered the opportunity to live and dwell independently, an 'active, meaningful existence in fellowship with others [189] and healthcare services adapted to their individual needs. [190] Still, promoting social security, preventing social problems, [191] ensuring quality and equality of healthcare services [192] and contributing to the best possible use of resources are other interest that must be given an equal weighting of consideration. [193] As in the most effective means, whether it is necessary to offer such services and whether this is in proportion to the risks involved will be the issue for scrutiny throughout the rest of this thesis. Detailed information about patients and potentially relatives and employees pose a risk of re-using information for

[183] Ibid, Main functions A-C.
[184] Ibid, Main function D.
[185] Ibid.
[186] GDPR, Article 5 (1)(b).
[187] HCSA, Section 1-1 (1).
[188] Ibid, Section 1-1 (6).
[189] Ibid, Section 1-1 (3).
[190] Ibid, Section 1-1 (5).
[191] Ibid Section 1-1 (2).
[192] Ibid, Section 1-1 (4).
[193] Ibid, Section 1-1 (7).

other or new and often incompatible purposes. This requires knowledge and awareness of data responsibility, privacy principles, and the legal use of sensitive information.

3.2.2 Legal basis

As controller that process data for their purposes, RoomMate shall commit to general compliance with the requirements in the GDPR. RoomMate relies on consent, the performance of a contract, or that the information is necessary to fulfil other legal obligations. They also justify grounds for processing based on legitimate interest. This condition always requires a balancing of interests in favour of the rights and freedoms of the data subject.[194] For example, personal data such as a name, e-mail or phone number may be processed because it is necessary information for the legitimate interest of RoomMate AS to provide customer support. [195] For the performance of a contract, this means that the contract cannot possibly be fulfilled unless personal data is processed. As the scope of this paper is mainly concerned with the municipality's overall responsibility and obligations, RoomMate's compliance with Article 9 for their purposes will not be assessed further.

Before intervening in a person's private sphere, one should guarantee grounds as a justification for doing so. The same principle applies to the municipality as they will be deploying RoomMate in the private room of elderly patients to provide enhanced healthcare services. For the municipality, the threshold for relying on a legal basis should be high as it is a public authority, and it cannot rely on legitimate interest. [196] A distinction between the need for a legal basis is required in two healthcare circumstances: a legal basis for *the provision* of healthcare services, namely the legitimate use of RoomMate and one for *the processing* of personal data and data concerning health.

3.2.3 Consent

All healthcare providers who process or have access to health information is subject to a duty of confidentiality. Legal grounds for processing necessary and relevant information [197] lies inherently in healthcare personnel's commitment to document [198] and provide primary healthcare

[194] GDPR, Article 6 (1)(f).
[195] RoomMate.no. "RoomMate as Personvern Policy." https://www.RoomMate.no/personvernpolicy/.
[196] Ibid, Article 6 (1), para. 2.
[197] Health Personnel Act, Section 40.
[198] Ibid, Chapter 8.

services. [199] Any processing of information outside of what is needed and appropriate would require a second legal basis, usually found in legal authority or obligation or from the consent given by the patient. As the municipality is the controller who decides the purpose for processing, it is also their role to consider approval. By default, the basis used for processing health data from using RoomMate would be consent to the use given by the patient. [200] However, issues emerge if the patient lacks the cognitive ability to provide consent. In this case, the next of kin or the relative should be involved to assess whether the patient would likely consent to this use or not. If no relatives are concerned, there should be appointed a guardian that acts on behalf of the ward to perform and make decisions in their best interests. [201] If consent cannot be relied upon, processing must be adequate to ensure an underlying objective. As processing personal data is prohibited, processing shall always ensure data minimisation insofar as it must be 'necessary. The interpretation of processing need not amount to 'indispensable' as the only way of achieving the objective. Still, it must be the most effective way to achieve the intended purpose. [202] Thus, a key criterion to show necessary processing entails assessing its effectiveness to ensure the underlying goal and whether a possibility to use other less intrusive means exists.

3.2.4 Vital interest, substantial public interest, or provision of social care

Article 9. Lit. C, lit. G, and lit. H could be relevant legal grounds for processing. A vital interest can be interpreted as 'essential for life', [203] effectively a high threshold, but appropriate as a lack of healthcare may result in loss of life for elderly patients. For 'substantial public interest', this needs a legal authority that provides 'suitable and specific' measures such as 'professional secrecy', which might protect confidentiality. Whereas lit. C allows for processing of data concerning health for the protection of 'vital interests' of data subjects who lack consent competence, lit. H could be triggered where processing is done to assess 'the provision of health or social care or treatment or the management of health or social care systems and services. [204]

---

[199] Ibid, Section 4, para.1.

[200] (KS), "Velferdsteknologiens Abc."

[201] Lov 25.mars 2010 nr.9. Lov om vergemål ver-gemålsloven) [The Guardians-hip Act], Section 20.

[202] Case C-524/06 *Huber v Bundesrepublik Deutschland.*

[203] GDPR, Recital 46.

[204] Ibid, Article 9 (2)(h).

3.2.5 Legal obligation

For those who cannot consent or show resistance to the RoomMate technology, a legal obligation could be relied upon as a basis for necessary processing. GDPR Article 9 lit. B, deals with 'obligations' and 'specific rights' of either controller and data subject, specifically in the field of 'social security and social protection law'. [205] For a legal obligation to be relied upon, the necessity criterion assumes that processing must be necessary to comply with the obligation. This will be the topic for analysis on relevant provisions in the following section.

3.2.6 Legal grounds for the use of RoomMate

3.2.6.1 The main rule of consent

The Norwegian Directorate of Health has specified that *tacit consent* is satisfied to use the RoomMate solution. [206] However, if the patient cannot consent due to a diagnosis, such permission does not suffice as the legal basis must be from statutory authority. [207] For patients diagnosed with mental disability who cannot consent or refuse the use of 'invasive warning systems with technical devices' [208] or 'technical facilities for notification and localisation', [209] healthcare providers need a supplementary legal basis to implement RoomMate.

Based on values of autonomy, self-determination and integrity, a patient shall have the option to accept or refuse the provision of healthcare services voluntarily and shall never be forced. [210] Chapter 4 of PURA provides rules on consent to health care. The main rule is that healthcare for adults can only be provided with the patient's consent unless there is a legal authority or another legal basis to offer the service without permission. [211] For consent to be valid, the patient must be given necessary information regarding their health status and

---

[205] GDPR, Article 9 (b).

[206] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.

[207] Direktoratet for e-helse Helsedirektoratet, Normen og PA Consulting, "Kvikk-Guide Til Behandling Av Helse- Og Personopplysninger Ved Bruk Av Velferdsteknologi. Nasjonalt Velferdsteknologiprogram," (2019).

[208] HCSA, Section 9-2 para. 2.

[209] PURA, Section 4-6 a para. 1.

[210] Ibid, Section 4-1 and Section 4A-1.

[211] Ibid, Section 4-1.

healthcare content. [212] The patient has a right to revoke consent and kept informed about the effects of a lack of healthcare. [213]

Arguably, when a patient agrees to healthcare, they implicitly also agree to measures implemented by the municipality in their provision of services. Thus, consent may be given either expressly or tacitly. [214] Tacit consent can be relied upon if, based on the patient's behaviour and circumstances, they are likely to accept the health care. [215] The exceptions deal with patients diagnosed with a mental disability [216] or who cannot otherwise consent. Consent can be given explicitly or implicitly. [217] Implicit consent is valid if the patient would likely accept the healthcare offer, considering the individual's actions and surroundings. [218] Some patients may initially show signs of resistance to the use of a GPS tracker or surveillance. However, the interest to own health and safety will likely outweigh patient's fear if they understand the objective of the seemingly invasive measure. In 2016, Oslo municipality deployed medical dispensers and issued consent declarations to gain written consent from patients. [219] However, this was swiftly disregarded due to the strenuous process of communicating a complex set of rules to patients with mental disabilities; an issue written declaration could not solve.
Nevertheless, by fostering continuous training and education of staff, patients can more easily enforce their right to gain information adapted to their needs. [220] The municipality creates information material to simplify the data and ensure the users have access to relevant information for their benefit. However, more robust protection is required for patients who lack the essential requisites for understanding this.

3.2.6.2 Issues of consent competence and resistance

Consent requires that a person must be able to understand what they are agreeing or refusing to. [221] This necessitates understanding the consequences of agreeing or opposing to

---

[212] PURA Section 4-1 para.1.
[213] PURA, Section 4-1 para.2.
[214] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.
[215] PURA, Section 4-2, para.1.
[216] HCSA Section 9-2 para.1.
[217] PURA, Section 4-2.
[218] PURA, Section 4-2.
[219] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.
[220] PURA, Section 3-1.
[221] (KS), "Velferdsteknologiens Abc."

RoomMate used as part of healthcare services and an ability to resonate relevant information and make a choice between the options given. As risks of compulsion towards patients with mental disabilities can have detrimental effects, explicit or tacit consent cannot, therefore, serve as the only legal basis. In the case of patients who lack the competence to consent, the provision in PURA will apply. Suppose the patient refuses to receive treatment or technology, meaning that through behaviour or use of words, the patient declines the offer of healthcare or technology. In that case, the healthcare provider must respect the autonomous choice of the patient. [222] How the resistance is expressed is not decisive as any sign of opposition is enough. [223] In many instances, this hinges on an interpretive evaluation of the reactions and requires knowledge about the patient's circumstances.

3.2.6.3 HCSA Section 9-2 [224]

When used for patients with a diagnosed mental disability, invasive warning systems shall consistently be recognised as a force or coercive measure. [225] The RoomMate technology can be considered as 'use of force' or 'coercive measure' [226] given that it falls within the category of 'invasive warning systems with technical devices'. [227] Suppose the municipality implements RoomMate with patients diagnosed with a mental disability. In that case, this requires an application to the County Governor [228] to assess and make a formal decision on the legitimate need. [229] As RoomMate is a tool for workers to perform more effective and even less invasive tasks, current law could be a disproportionate hindrance to accommodating the patient's best interest and healthcare. As the municipality has an incentive to implement RoomMate in the bedrooms of the patient's home, a potential reform or relaxation on the current provisions on use of force in healthcare could create issues for this vulnerable patient groups as compulsion can occur. Still, strict limitations and duties for care providers exist elsewhere in legislation.

---

[222] PURA, Section 4-6 a, para. 3.
[223] (KS), "Velferdsteknologiens Abc."
[224] HCSA, Section 3-2 and Section 9-2.
[225] HCSA, Section 3-2 and Section 9-2.
[226] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.
[227] HCSA, Section 9-2, para. 2.
[228] In Norwegian, 'Statsforvalteren'.
[229] Interview with employees in Helseetaten, Oslo municipality. 26 April 2021.

3.2.6.4 PURA Section 4A-3 and 4-6 a

As seen above, current law protects patients with medical disabilities and their right not to be subject to RoomMate as it is a recognised use of force. Following Section 3.1.1, it may be assumed that the provision applies to RoomMate as an 'invasive technology'. Further, Section 4-6a permits the municipality to decide on 'notification and localisation technology' to patients without competence to give consent. [230] The differences between the two provisions are that HCSA Chapter 9 is diagnosis-specific. In contrast, Section 4-6a in PURA engages patients who cannot consent, necessitating a reasoned, written and continuous assessment upon the service provider. [231]

Section 4-6 a seems to set a higher threshold for the provision in HCSA, as the measure to implement RoomMate for those who lack consent competence requires assessing three criteria. Further, the action must be necessary to prevent or limit the risk of *harm* to the patient and should be in their interest. [232]

i. Is the measure reasonably proportionate to the relevant risk?
ii. Is the measure considered the least invasive option?
iii. Is it likely that the patient would have permitted the measure? [233]

The ordinary meaning of 'risk of harm' to the patient' entails that the measure must be necessary to protect the patient against harm. Given that the risk must be reasonably proportional to the measure, each risk should be assessed distinctly. The risk of falling could cause harm, and RoomMate could be a measure to prevent or limit such a risk. Still, whether it is the least invasive option should also be considered, as is the patient's opinion. By the wording of Section 4-6 lit. A., RoomMate would be a lawful measure insofar as it can prevent or limit harm or the risk of harm to the patient. A reason is the ability to automatically detect critical events the patient is exposed to, such as a fall, and notify the care provider upon this event. One could argue that 'but for the RoomMate technology, the patient risks harm to own health' because healthcare might not act upon the fall quickly. Thus, it can prevent and limit the risk of

[230] PURA, Section 4-6 a, para. 1.
[231] Ibid, para. 3.
[232] Ibid, para. 2.
[233] Ibid.

falling, including both the physical and physical consequences of the incident. Nevertheless, the necessity criterion and the inclusion of 'relevant risk' raises several questions regarding the risk in the context of the individual patient and the use of RoomMate. Also, the fact that the measure should be in the patient's interest would suggest that this is not the main priority as the prevention or limitation to the risk of harm to the patient is. Moreover, the provision states that the healthcare service *may* decide to implement such devices and is not obligated to the municipality. This can nevertheless be recognised as a sufficient legal basis for the municipality to implement the RoomMate technology and patients who cannot give valid consent, [234] such as patients with dementia or reduced cognitive functions. [235] Regarding the third criterion, information from the patient's closest relatives should be obtained about what the patient would have wanted. [236]

3.2.6.5 Use of force and resistance

If a patient without the capability to consent also oppose the use of RoomMate, it might not be lawful for implementation. A sign of resistance can be interpreted as an expression of the conflict between two desires. [237] This entails that health personnel play a crucial part as their experiences and knowledge of the patient will matter for their discretionary assessment. In any case of doubt, it shall always be assumed that the patient opposes. [238] If the patient objects to the use, Section 4A may be engaged. [239] This chapter aims to provide necessary healthcare to prevent significant health damage and *prevent and limit the use of force*. [240] If the conditions in Section 4A-3 are fulfilled, healthcare can be offered with power or other measures to circumvent the patient's resistance. [241] The provision's wording applies distinctly to 'significant health damage', not mere 'harm' as in Section 4-6- A. The natural meaning of both includes harm, both mental and physical.

---

[234] PURA, Section 4-3.

[235] PURA, Section 4-6 a.

[236] Ibid, para. 3.

[237] Bjørn Henning Østenstad, *Heimelsspørsmål I Behandling Og Omsorg Overfor Psykisk Utviklingshemma Og Aldersdemente: Rettslege Og Etiske Problemstillingar Ved Bruk Av Tvang Og Inngrep Utan Gyldig Samtykke*, vol. 1 (Fagbokforlaget, 2011).

[238] Prop. 90 L (2012-2013) Endringer i pasient- og brukerrettighetsloven mv. (bruk av varslings- og lokaliseringsteknologi)" [Changes in the Patient and User Rights Act (use of alarm and location technology - Proposition on legislation to the Storting]. pt.7.3.3.

[239] PURA, Section 4-6 a para. 3.

[240] PURA, Section 4A-1.

[241] PURA, Section 4A-4.

In situations where use of force would be legitimate, but knowledge from the patient is impossible to rely upon, gaining consent can be a significant hindrance to offer necessary healthcare. Nevertheless, a legal three-part test sets out qualifications that must be established. This requires that (i) the healthcare must be necessary, (ii) the measures must be proportionate to the patient's need for care and (iii) a failure to provide such care could cause *significant health damage* to the patient.[242] If these criteria are met, then deciding to implement invasive technology *can* establish a legitimate adoption of RoomMate. However, this sets a very high threshold as 'significant health damage' to the patient is an unlikely result of using RoomMate. On the other hand, this is an actual risk regarding the elderly and the fall problematisation. [243] The meaning of 'significant health damage' would mean that the patient is at risk of 'health damage of significant extent or with other serious consequences [244] Specific forms of manipulation and use of force are often relied upon in the relationship between care worker and patients. This is likely why the provision in 4A-3 can be relied upon to justify the provider's need to take necessary actions in the patient's well-being and interest. For example, to prevent or reduce malnutrition, it may be acceptable that a worker feeds a patient who initially refuses the feeding. Health personnel might also sneak medication into the patient's diet without being aware to ensure they take their medication. [245] This is still a use of force as the patient is deprived of their choice to refuse. The case of RoomMate is different, seeing as a lack of this measure would less likely constitute a severe risk such as malnutrition. The measure to implement RoomMate could be helpful in this sense if healthcare providers can provide quicker and more effective services and show proactiveness to prevent or reduce risks of such consequences. The predicament here turns to reconcile the fundamental freedoms of self-determination and privacy and the health and safety of the individual. RoomMate cannot prevent falling itself, but it can avoid the aftermath and further damage resulting from the fall. Also, the obligation of the healthcare service and the professional responsibility of personnel to make discretionary assessments based on their expertise is essential. To impose RoomMate upon

---

[242] PURA, Section 4A-3.

[243] NOU 2011: 11 «Innovasjon I omsorg» [Innovation in care].

[244] Ot.prp. nr. 64 (2005–2006) "Om lov om endringar i pasientrettslova og biobanklova (helsehjelp og forsking – personar utan samtykkekompetanse)" [About the law on amendments to the Patient Rights Act and the Biobank Act (health care and research - persons without consent competence)], pt.8.

[245] Odland, "Hjemmelen for Å Bruke Varslings- Og Lokaliseringsteknologi Som Helsehjelp Til Mennesker Med En Demensdiagnose. En Drøfting Av Reguleringene I Pasient- Og Brukerrettighetsloven Kapittel 4a Og § 4-6 A.."

patients with mental disabilities or who cannot consent and show signs of opposing the use would constitute an apparent violation of the patient's right to self-determination and integrity. Issues are further complicated where the law is ambiguous and tougher to enforce. A legal obligation following the requirement of professional conduct, patient safety and quality involves that an action against the patient's will must satisfy a need for health care in a proportionate and responsible manner. [246] If using RoomMate or processing health data is no longer necessary, processing should end immediately as it will no longer be proportionate. If the necessity criterion is not practiced, elderly patients may be exposed to a greater number of risks to violations of their fundamental rights and freedoms.

[246] The Health Personnel Act.

4 Balancing of interests: Is DPbDD the solution?

To what extent is 'data protection by design and by default' (GDPR, Article 25) an effective and appropriate mechanism for balancing various considerations of the elderly's health, safety, and privacy? The implementation of the RoomMate technology gives rise to a tension between health and safety on the one hand and 'privacy' on the other. This Chapter is dedicated to addressing any gaps resulting from the RoomMate implementation and assess how DPbDD operates as a mechanism to balance the competing interests. As one of the genuinely new provisions in the GDPR, Article 25 could be seen as part of the growing global discourse on PbD and SbD and offers an innovative attempt to oblige data controllers to keep privacy-related interests as a key goal when defining system requirements. [247] However, it is primarily up to the controllers to take proactive measures in complying with Article 25. [248]

As DPbDD was set in the requirements specification of the municipality's tender call for welfare technology, RoomMate was expected to have implemented default settings at the most privacy-friendly level. [249] The effects of this will serve the municipality's often speedy and costly procurement of innovative welfare technology, as risks to data subjects' privacy and safety can be reduced and mitigated. This could ultimately gain trust in the healthcare service and allow resources to be allocated more efficiently, saving time and costs for all actors involved. Showing transparency and management commitment in the initial design and software development will likely be advantageous to gain trust and feeling of safety and eagerness in users' interaction with RoomMate.

4.1 Strategies

Organizations that take data protection issues seriously build trust. Thus, robust data protection measures can be used to gain a competitive advantage on the market. The RoomMate system was designed from the ground up, focusing on privacy and data security, in line with Article 25. Following input from the DPA, basic design choices were made for data security and privacy. Nevertheless, there are concerns relating to the high level of invasiveness and

[247] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive – DPD) did not have an equivalent provision to Article 25.

[249] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

surveillance of the elderly in the privacy of their bedrooms at home. More importantly, elderly patients often lack the basic understanding of ICT that will massively impact their acceptance, enforcement of rights to information and capability to consent to the RoomMate technology. Both ENISA and the Norwegian DPA recommend requirements for the design and process of technology by distinguishing between data and process-oriented strategies. [250] *Data-oriented* strategies are concerned with the processing of data. This highlights lawful, fair, and transparent processing principles to ensure data minimization and purpose limitation. [251] Ideally, settings are set at the most privacy-friendly level by default without the user's need to opt-out of sharing personal data. This is in line with the principle of data minimisation to ensure processing on a 'need-to-know' as opposed to a 'nice-to-know basis. *Process-oriented* strategy is about upholding the data subjects' rights in the design. [252] This includes the requirement to correctly inform users on how the technology functions and how personal data is processed, give data subjects control over their data with easy access to give or withdraw consent and delete or update personal information themselves. [253]

4.1.1 Data-oriented

RoomMate can contribute to increased security and privacy for elderly patients and their relatives. When public authorities act as a paternalist on behalf of citizens, measures on providing healthcare services should interfere only to a proportionate and necessary extent with the autonomy and integrity of individuals. This means that the least invasive measure present must be implemented to achieve the purpose to safeguard patient's autonomy and avoid arbitrary interference with their legal and private sphere. To implement a measure against the patient's will requires a fulfilment of an underlying objective to prevent and limit the risk of harm and damage to the patient. Determining what the least or most intrusive option is not apparent. It will hinge on a proportionality and necessity assessment for each patient based on their will, context and need for care. According to the provisions in PURA Section 4A, a measure must be proportionate to the patient's need for healthcare, and this requires a continuous evaluation. [254] If there is a great need for healthcare provision, adopting invasive technology may be

---

[250] European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design – from Policy to Engineering," (2014).

[251] GDPR, Article 5 (1)(b)-(c).

[252] (DPA), "Software Development with Data Protection by Design and by Default."

[253] (ENISA), "Privacy and Data Protection by Design – from Policy to Engineering.", 20-22.

[254] Ot.prp. nr. 64 (2005–2006), pt. 8.

proportionate to serve the patient's health and safety. RoomMate's use may not be proportionate where the need for healthcare is not so imminent. Surely, invasive technology should never be used as a sole means to provide health and care services. However, deciding on the least or most intrusive means used by health personnel to offer high-quality services and efficiency is not apparent and will depend on the level of interference with the individual's privacy. [255] RoomMate can replace regular physical supervision to an extent and will not necessarily always be the most intrusive means. It may be just as invasive, or more, if an employee follows and physically monitors the patient as it would be if this is done virtually. In the same way, it can be equally disturbing if a worker checks in on the patient physically, as it is for a sensor to register their movements.

4.1.2 Process-oriented

Processing health data and the use of RoomMate as an invasive measure can be lawful; it is equally important to assess the significance of the process-oriented strategy, namely how data subjects' rights can be protected in the design. RoomMate was given a high score on the quality of their service since they could offer a card for de-activation [256] which means that the sensor and alerts can be deactivated if the patient is away on holiday, have visits from family/friends or otherwise wish to deactivate the sensor and maintain a level of control. [257] Nevertheless, it is likely that the patient does not understand this function or that the worker or another person forgets to make use of this. Also, each digital supervision is limited to sixty seconds by default, and upon configuration the user may decide whether 'anonymized' or detailed images are shown or not. [258] Nevertheless, as mentioned in the previous Chapter, there are many issues on the continuous complexity of ensuring effective anonymisation. The risks of interconnected devices in the healthcare sector could likely impose unforeseen challenges to protect privacy considerations. Also, the municipality must comply with universal design principles, reflected as a minimum requirement in the tender calls [259] as well as in regulation on universal design. [260] The municipality is responsible for demonstrating compliance with

---

[255] Ibid.

[256] RoomMate, "Roommate, Avstillingskort, Rev B," (2020).

[257] Evaluation requirement with value 4 in ibid, pt. 1.4.

[258] (SSA-K), "Appendix 1: Customer Requirements Specification. Digital Supervision ".

[259] Ibid.

[260] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Dir 2016/2102).

new rules [261] in the new Directive passed as part of the EEA Agreement [262] and likely relevant for application as they offer services to citizens in the form of ICT solutions. This might lead to an increased user acceptance and understanding of health staff in their interaction with the solution. Further, RoomMate's invasiveness with patient's privacy could outweigh certain considerations of health personnel. Nevertheless, the municipality as an employer is obliged to facilitate that RoomMate constitutes the least possible burden for health personnel in their work tasks, as the use includes audio and image. [263] This involves implementing various forms of measures in the workplace to ensure that the employees are comfortable with the help of RoomMate. The data controller is obliged to document compliance with relevant privacy considerations, e.g., by a Privacy Policy with a demonstration of implemented measures. The municipality is also obligated to provide relevantly and adapted information to the data subjects about image and audio recording. [264] At a minimum, the municipality should also establish routines to manage privacy consideration on behalf of patients and health personnel being employees. This should include a personnel handbook or similar on the use and personal data collected by RoomMate, how it functions so the employees can safeguard their own and patients' rights. [265]

[261] Ibid.

[262] As of 5 February 2021.

[263] (Normen), "Veileder for Bruk Av Video, Lyd Og Bilde I Helse-Og Omsorgssektoren Versjon 2.0."

[264] Ibid., 12.

[265] Ibid.

5 Conclusion

This paper has utilized key operative provisions in binding legal frameworks and industry norms and standards to assess challenges related to adopting innovative welfare technology in the provision of healthcare services to elderly patients and users. The introduction put forward issues of an ageing population and a decrease in the needed labour force. Further, the respective RoomMate technology was used as an example to study the legal problems and establish main possibilities and pitfalls associated with the municipal healthcare institutions' procurement of invasive welfare technology. Specific problems relating to anonyisation techniques and consent competence were given a particular focus. Lastly, the potential of DPbDD as a mechanism to ensure lawful processing and reduce and mitigate risks was topic for discussion in Chapter 4.

For many patients, RoomMate could be a safe and less intrusive measure than physical supervision. For others, it may not. Nevertheless, the general use raises several issues regarding adequate anonymization and necessary actions to ensure healthcare providers and personnel ability to offer services. Even if a patient is not directly identified, data is not necessarily anonymous, as the mere possibility of identification is enough for the data protection rules to apply. [266] The fact that a person is identifiable entails that identification is possible. This is sufficient to suggest that the anonymisation techniques used by RoomMate may not amount to personal data rendered truly anonymous as the WP29 sets a high threshold in data needing to be impossible to reverse-engineer. [267] Further, the possibility to deanonymize detailed images and sound detected by the RoomMate sensor could suggest that the collection of personal data may not have been effectively anonymous in the first place. With the increased advancement in digitalization, it is possible to analyse patterns and conduct behaviour analysis and profiling of individuals. In many cases, this will effectively gather more personal data than its original purpose was for, thus constituting a highly invasive measure to the individual's privacy. Moreover, the use of image and audio in the healthcare service demands processing many categories of personal data. Already, vast amounts of information gathered in this context are

[266] Voigt and von dem Bussche, *The Eu General Data Protection Regulation (Gdpr): A Practical Guide*.
[267] (WP29), "Opinion 05/2014 on Anonymisation Techniques ".

kept in confidential electronic medical records that often needs to be shared and used across institutions and professionals. Whereas a traditional video camera will detect detailed information about the individual's movements, facial expressions, and surroundings, the RoomMate solution utilises sensor technology based on IR light analysed by the sensor's computer to expose three types of real-time images [268] and sound from the patient's bedroom. The function to remotely monitor patients at risk of health damage can be highly contributory in many aspects to safeguard patient's health and safety and provide quicker and more effective healthcare. Still, sufficient guarantees to ensure data privacy and security interests are also crucial as increased digitalisation requires increased protection.

There are many risks of using technology that involves a combination of camera surveillance, sensor technology and audio recording; however, the gains could unarguably outweigh these costs if managed appropriately. When used in combination with elderly and often vulnerable patients with mental disabilities or incapability to consent, RoomMate may conflict with the patients' rights. However, many risks can be tolerated as mechanisms and strategies to reduce and mitigate such risks exist. Ultimately, responsibility must be anchored at the top leadership level of healthcare agencies, demonstrating compliance with laws and fostering effective ISMS to nurture a sustainable culture for security management and handle deviations. The municipal leadership plays a crucial part as mediators between users and ICT. They are responsible for establishing a legitimate purpose and lawfulness of processing health data and implenting proactive measures to ensure a trustworthy and well-functioning healthcare service. This means protecting both healthcare recipients and providers and their privacy and safety in interaction with invasive welfare technologies. As citizens grow older and increasingly prone to life-threatening risks, they should expect, trust and rely on high-quality healthcare services using welfare technology to assist healthcare personnel in performing their crucial tasks. Many actors are involved in this process which necessitates designating specific roles and responsibilities. It is the responsibility of the municipal leadership as the data controller to show a proactive approach in line with DPbDD. The benefits of doing so will ensure a higher level of protection of user-centred and efficient healthcare services and reduce risks to arbitrary interference with individual's privacy and integrity as fundamental pillars of the digital welfare state.

[268] Chapter 2, Section 2.1.1.

Table of reference

Norwegian legal sources

Statutory law

2018	Lov 15.juni 2018 nr. 38. Lov om behandling av personopplysninger [The Personal Data Act]
2014	Lov 20.juni 2014 nr. 43. Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) [Personal Health Data Filing System Act]
2014	Lov 20. juni 2014 nr. 42. Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) [the Health Records Act]
2013	Forskrift 21. juni 2013 nr. 732 om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger [The Universal Design of ICT Solutions Regulation]
2011	Lov 24. juni 2011 nr. 30. Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven) [The Health and Care Services Act - HCSA]
2010	Lov 25.mars 2010 nr.9. Lov om vergemål vergemålsloven) [The Guardianship Act]
2006	Lov 19.mai 2006 nr.16. Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova). [Act relating to the right of access to documents held by public authorities and public undertakings - Freedom of Information Act]

1999	Lov 2.juli 1999 nr. 63. Lov om pasient- og brukerrettigheter (Pasient- og brukerrettighetsloven) [The Patient and User Rights Act - PURA]
1999	Lov 2. juli 1999 nr. 64. Lov om helsepersonell m.v. (helsepersonelloven) [the Health Personnel Act]
1992	Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven) [Act implementing the main part of the Agreement on the European Economic Area etc. into Norwegian law – The EEA Act]
1967	Lov 10.februar 1967 nr. 00. Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) [Act relating to procedure in cases concerning the public administration - Public Administration Act].
1814	Lov 17.mai 1814 Kongeriket Noregs grunnlov (Grunnlova) [The Norwegian Constitution]

Preparatory works

NOU 2018:14: «IKT-sikkerhet i alle ledd» [ICT Security at all stages].

NOU 2011:11: «Innovasjon i omsorg» [Innovation in care].

Prop. 90 L (2012-2013) Endringer i pasient- og brukerrettighetsloven mv. (bruk av varslings- og lokaliseringsteknologi)" [Changes in the Patient and User Rights Act (use of alarm and location technology - Proposition on legislation to the Storting].

Meld. St. 9 (2012–2013) "En innbygger – en journal" [One citizen – one health record].

Ot.prp. nr. 64 (2005–2006) “Om lov om endringar i pasientrettslova og biobanklova (helsehjelp og forsking – personar utan samtykkekompetanse)” [About the law on amendments to the Patient Rights Act and the Biobank Act (health care and research - persons without consent competence)].

International legal sources

EU law

Dir 2016/2102	Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies.
Reg 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
Dir 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, 0031–0050 (DPD).
1992	The EEA Agreement on the European Economic Area original agreement signed 2 May 1992 (The EEA Agreement)

Case law

The European Court of Human Rights (ECtHR)

Application no. 20511/03 Judgement of 17 July 2008 (*I v. Finland)*	ECLI:CE:ECHR:2008s:0717JUD002051103 <http://hudoc.echr.coe.int/eng?i=001-87510>

Court of Justice of the European Union (CJEU)

Case C-434/16 *Peter Nowak v Data Protection Commissioner*	ECLI:EU:C:2017:994 <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0434>
Case C-131/12 *Google v Spain*	ECLI:EU:C:2014:317 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>
Case C-524/06 *Huber v Bundesrepublik Deutschland*	ECLI:EU:C:2008:724 < https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62006CJ0524>
Case C-465/00 *Rechnungshof and others*	ECLI:EU:C:2003:294 <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62000CJ0465>
Case C-101/01 *Lindqvist*	ECLI:EU:C:2003:596 < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101&qid=1621028747360>

Literature, guidance, reports and recommendations

(Digdir), Norwegian Digitalisation Agency. "Internkontroll I Praksis - Informasjonssikkerhet [Information Security Management System in Practice] (Version 1.5) ". https://internkontroll-infosikkerhet.difi.no/.

———. "Internkontroll I Praksis – Informasjonssikkerhet. Grunnleggende Begreper [Information Security Management Systems in Practice. Basic Concepts]."

(DPA), Datatilsynet. "Anonymisering Av Personopplysninger. Veileder." 2015.

———. "Software Development with Data Protection by Design and by Default." 2017.

(EC), European Commission. "The 2021 Ageing Report: Underlying Assumptions and Projection Methodologies." 2020.

(ENISA), European Union Agency for Network and Information Security. "Privacy and Data Protection by Design – from Policy to Engineering." 2014.

(KS), Kommunesektorens Organisasjon. "Velferdsteknologiens Abc." (2016).

(Normen), Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. "Veileder for Bruk Av Video, Lyd Og Bilde I Helse-Og Omsorgssektoren Versjon 2.0." Direktoratet for e-helse, Helse- og omsorgsdepartementet, 2021.

(SSA-K), Norwegian Government's Standard Terms and Conditions for IT Procurement. "Appendix 1: Customer Requirements Specification. Digital Supervision ", 2018.

(SSB), Statistics Norway. "1 Av 5 Nyutdanna Sykepleiere Jobber Ikke I Helsetjenesten." https://www.ssb.no/helse/artikler-og-publikasjoner/1-av-5-nyutdanna-sykepleiere-jobber-ikke-i-helsetjenesten.

(WP29), Article 29 Data Protection Working Party. "Opinion 4/2007 on the Concept of Personal Data, 20 June 2007 ('Wp 136')."

———. "Opinion 05/2014 on Anonymisation Techniques ", 2014.

Cavoukian, Ann. "Privacy by Design - the 7 Foundational Principles." Information & Privacy Commissioner Ontario, Canada, 2009.

Christopher, Kuner, A. Bygrave Lee, Docksey Christopher, and Drechsler Laura. *The Eu General Data Protection Regulation (Gdpr) : A Commentary.* [in English] [Place of publication not identified]: OUP Oxford, 2018. Book.

Cozza, Michela, Lucia Crevani, Anette Hallin, and Jennie Schaeffer. "Future Ageing: Welfare Technology Practices for Our Future Older Selves." *Futures : the journal of policy, planning and futures studies* 109 (2019): 117-29.

Dworkin, Gerald. "Paternalism." *The Monist* 56, no. 1 (1972): 64-84.

Esayas, Samson. "The Role of Anonymisation and Pseudonymisation under the Eu Data Privacy Rules: Beyond the 'All or Nothing' Approach." *European Journal of Law and Technology* Vol 6, No 2. (Oct 15 2015).

Helsedirektoratet, Direktoratet for e-helse, Normen og PA Consulting. "Kvikk-Guide Til Behandling Av Helse- Og Personopplysninger Ved Bruk Av Velferdsteknologi. Nasjonalt Velferdsteknologiprogram." 2019.

Helseetaten. "Velferdsteknologi." https://www.oslo.kommune.no/getfile.php/13313507-1549878854/Tjenester%20og%20tilbud/Helse%20og%20omsorg/Fag%20og%20kompetanse%20-%20helse%20og%20omsorg/Velferdsteknologi%20%20brosjyre.pdf.

Høringssvar - Nou 2018: 14 Ikt-Sikkerhet I Alle Ledd Og Utkast Til Lov Som Gjennomfører Nis-Direktivet I Norsk Rett, 21.03 2019.

ISO. "Iso 27001:2013 Information Security Management System - Isms." 2013.

Jacobsen, Dag Ingvar. *Hvordan Gjennomføre Undersøkelser? : Innføring I Samfunnsvitenskapelig Metode.* 3. utg. ed. Oslo: Cappelen Damm akademisk, 2015.

Langskov, Marie and Jørgensen, Tina. "Technology and the Welfare System – a Discussion Paper." In *The National Political Conference on Welfare Technology* 8. Copenhagen, Denmark: European Commission (EC), 2008.

MacKay, Douglas. "Basic Income, Cash Transfers, and Welfare State Paternalism." *The journal of political philosophy* 27, no. 4 (2019): 422-47.

Narayanan, A., and E. Felten. "No Silver Bullet: De-Identification Still Doesn't Work." 2014.

"Norm for Informasjonssikkerhet Og Personvern I Helse Og Omsorgstjenesten (Normen) ". edited by Helse- og omsorgsdepartementet Direktoratet for e-helse. normen.no 2020.

Normen. "Faktaark 46 - Personvern Og Informasjonssikkerhet Ved Tjenesteutsetting Av Kommunale Helse- Og Omsorgstjenester_5.0.Pdf."

———. "Veileder Informasjonssikkerhet Og Personvern Ved Bruk Av Velferdsteknologi 3.0.".

Odland, Ida Victoria Rullestad. "Hjemmelen for Å Bruke Varslings- Og Lokaliseringsteknologi Som Helsehjelp Til Mennesker Med En Demensdiagnose. En Drøfting Av Reguleringene I Pasient- Og Brukerrettighetsloven Kapittel 4a Og § 4-6 A." Master thesis, University of Bergen, 2018.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA law review* 57, no. 6 (2010): 1701-77.

Østenstad, Bjørn Henning. *Heimelsspørsmål I Behandling Og Omsorg Overfor Psykisk Utviklingshemma Og Aldersdemente: Rettslege Og Etiske Problemstillingar Ved Bruk Av Tvang Og Inngrep Utan Gyldig Samtykke.* Vol. 1: Fagbokforlaget, 2011.

Purtova, Nadezhda. "The Law of Everything. Broad Concept of Personal Data and Future of Eu Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (2018/01/02 2018): 40-81.

RNJ. "Roommate, Oversikt Personvern Og Datasikkerhet, Rev A." edited by RoomMate AS. Roommate.no, 2020.

———. "Roommate, Systemarkitektur, Rev E." roommate.no: RoomMate AS, 2021.

RNJ, TK. "Roommate, Installasjonsveiledning, Rev D." RoomMate AS, 2018.

RoomMate. "Roommate, Avstillingskort, Rev B." 2020.

RoomMate.no. "Roommate Anonymisert Tilsyn Og Pasientvarsling." https://www.roommate.no/roommate/.

———. "Roommate as Personvern Policy." https://www.roommate.no/personvernpolicy/.

———. "Roommate Nyheter Og Referanser." https://www.roommate.no/referanser/.

———. "Roommate Ofte Stilte Spørsmål – Faq." https://www.roommate.no/faq/.

———. "Roommate Systemet – Et Komplett Sykesignalanlegg." https://vimeo.com/525444389.

Skelton, D. A., C. Becker, S. E. Lamb, J. C. T. Close, W. Zijlstra, L. Yardley, and C. J. Todd. "Prevention of Falls Network Europe: A Thematic Network Aimed at Introducing Good Practice in Effective Falls Prevention across Europe." [In eng]. *European journal of ageing* 1, no. 1 (2004): 89-94.

Skullerud, Åste Marie Bergseng. "Personvernforordningen. Lovkommentar, Artikkel 4. Definisjoner, Juridika ".

———. "Personvernforordningen. Lovkommentar, Artikkel 25. Innebygd Personvern Og Personvern Som Standardinnstilling, Juridika."

Ulseth, Henrik and Teie Hellum, Petter. "Vurdering Av Helseetatens Etterlevelse Av Normens Krav Til Konfidensialitet Og Tilgangsstyring." Master thesis, University of Oslo, 2020.

"Velferdsteknologisk Knutepunkt (Vkp)." Direktoratet for e-helse, https://ehelse.no/velferdsteknologi/velferdsteknologisk-knutepunkt-vkp.

Voigt, Paul, and Axel von dem Bussche. *The Eu General Data Protection Regulation (Gdpr): A Practical Guide.* Cham: Cham: Springer International Publishing AG, 2017.

Zalta, Edward N. "Paternalism." Stanford, CA: Stanford University, 2013.