SMER
Society of Medical Education & Research

Society of Medical Education & Research

2024, Volume 4, Page No: 204-214
ISSN: 3108-5059

Asian Journal of Ethics in Health and Medicine

Ethical Considerations in Health Monitoring within the Armed Forces: A Dutch Case Study during the COVID-19 Pandemic

Tenzin Dorji[1]*, Pema Wangchuk[1]

[1]Department of Health Ethics, Faculty of Health Sciences, Khesar Gyalpo University of Medical Sciences, Thimphu, Bhutan.

***E-mail** ✉ tenzin.dorji@outlook.com

Abstract

Personal health monitoring (PHM) is rapidly evolving across multiple domains, including military contexts. Addressing the ethical aspects of PHM is crucial to ensure its responsible deployment and use among armed forces personnel. Most studies on PHM ethics have focused on civilian populations, leaving a gap in understanding the unique ethical challenges within military environments, where tasks, hierarchy, and operational conditions differ. This case study explores the perspectives and values of various stakeholders regarding the Covid-19 Radar app, a PHM tool used in the Netherlands Armed Forces. An exploratory qualitative approach was employed, involving semi-structured interviews with twelve military stakeholders. The investigation focused on engagement with PHM, reflections on its practical application and data handling, moral dilemmas encountered, and the perceived need for ethical guidance. The collected data were analyzed using an inductive thematic method. Analysis revealed three overlapping categories relating to PHM ethics: (1) core values, (2) moral dilemmas, and (3) external standards. Central values included data security, trust, and hierarchical structure, alongside several related ethical considerations. Some moral dilemmas were reported, but no widely shared dilemmas emerged, and participants generally did not express a strong demand for ethics support. The study identifies key values and provides insight into both experienced and anticipated moral dilemmas, emphasizing considerations for ethical support in military PHM. Certain values may expose military personnel to vulnerability when personal and organizational priorities conflict, while others may obscure aspects of ethical decision-making. Ethics support could help reveal and address these hidden ethical challenges, highlighting the armed forces' responsibility to carefully attend to the ethical dimensions of PHM.

Keywords: Ethical considerations, Armed forces, Health, COVID-19

Introduction

Smartwatches and other wearable devices are increasingly used to monitor health metrics, reflecting the rapid expansion of personal health monitoring (PHM). Examples include continuous glucose measurement, sleep tracking, fall-risk assessment, gait monitoring, ECG recording, and activity tracking. The global mobile health sector is projected to expand from USD 56.8 billion in 2022 to USD 130.6 billion by 2030, growing roughly 11% per year [1], driven by population aging, chronic disease prevalence, rising healthcare costs, personalized medicine trends, and the Internet of Things [1–4].

PHM refers to "any electronic device or system that longitudinally monitors and records data about a health-related aspect of a person's life" [5]. In civilian healthcare, PHM is applied in prevention (e.g., remote monitoring for congestive heart failure [6]), treatment (e.g., continuous glucose monitoring for diabetes), care facilitation (e.g., Covid-19 contact tracing [7]), and rehabilitation (e.g., post-stroke gait recovery [8]). It is also increasingly used recreationally and in occupational

Access this article online https://smerpub.com/

Received: 11 May 2024; **Accepted:** 21 August 2024

How to cite this article: Dorji T, Wangchuk P. Ethical Considerations in Health Monitoring within the Armed Forces: A Dutch Case Study during the COVID-19 Pandemic. Asian J Ethics Health Med. 2024;4:204-14. https://doi.org/10.51847/XV2L2pctU9

health, supporting fitness tracking and employee wellbeing programs [9]. Benefits of PHM include continuous data collection, pattern recognition, early detection of health issues, diagnostic support, and personalized lifestyle guidance [10].

In military settings, PHM has potential applications such as monitoring sleep in soldiers post-deployment using wrist actigraphy [11], assessing fatigue and physical strain through non-invasive physiological devices [12], and preventing exertional heat illness via biometric sensor systems [13]. Research in these settings has mostly examined technical feasibility, accuracy, and health outcomes.

However, PHM also raises ethical questions that extend beyond technical performance or cost efficiency [14]. These include concerns about privacy, autonomy, safety, appropriate data use, and the potential medicalization of personal or professional life [15, 16]. Ignoring these ethical considerations can reduce the benefits of PHM or even cause harm [15, 17].

Soldiers operate under military law, are embedded in a distinct military culture, and often serve in extreme or hostile environments. This unique context raises questions about whether—and to what extent—the ethical considerations surrounding personal health monitoring (PHM) in the armed forces differ from those in civilian settings. While prior research has examined PHM ethics in civilian healthcare [17–19] and its importance has been emphasized by some scholars [20], no studies specifically address the ethical aspects of PHM within military contexts. Consequently, this study focuses on exploring the ethical dimension of PHM among armed forces personnel. We define this ethical dimension as encompassing both implicit and explicit normative perspectives on the nature, characteristics, risks, and applications of PHM, as perceived by users and other stakeholders such as developers and policy advisors. These normative perspectives provide guidance on what is considered right or wrong, desirable or undesirable, and responsible or irresponsible, and can be expressed through experiences, attitudes, moral questions, rules, or agreements.

Understanding this ethical dimension can promote responsible PHM use within the military and other high-risk organizations, such as police or security services. Responsible use entails balancing operational objectives with the protection of soldiers' privacy and personal lives. The insights gained from this study can inform the development, deployment, and use of PHM tools in military settings, maximizing potential benefits while mitigating risks and safeguarding personnel from misuse. To investigate the ethical dimension of PHM in the military, we conducted an in-depth case study of the Covid-19 Radar app, which was implemented in a national reserve unit of the Netherlands Armed Forces. This study addresses two research questions: (1) which values do users and stakeholders consider important regarding the development, implementation, and use of Radar, and (2) what support needs do they express concerning the ethical aspects of PHM?

Radar was developed collaboratively by the Defence Health Organisation of the Netherlands Armed Forces and a civilian technology partner to monitor Covid-19-related military readiness and help limit SARS-CoV-2 transmission among personnel. The mobile application collected daily symptom data through a questionnaire based on guidance from the Netherlands National Institute for Public Health and the Environment [21]. Respondents received personalized advice, indicating whether they should report for duty or self-isolate and consult a military physician. Aggregated data also provided military physicians with insights into symptom trends within units, supporting their advisory role to commanders. From November 2020 to April 2021, Radar was trialed in a national reserve unit, selected for its willingness to participate without disrupting regular duties. Soldier participation was voluntary and anonymous, making this pilot one of the first military PHM implementations in the Netherlands and a valuable case for studying ethical dimensions.

Materials and Methods

Study design

We employed a qualitative, exploratory approach using semi-structured interviews, enabling participants to discuss the values, norms, and moral questions they associated with Radar, as well as any dilemmas encountered.

Data collection

The study focused on a national military reserve unit with 143 personnel at the time, of whom 78 took part in the Radar trial. Reservists perform military duties alongside civilian jobs or studies. The entire unit received personal invitations to join the study. Additional stakeholders were identified through purposive and snowball sampling and invited individually.

Twelve participants—four users and eight stakeholders—were included. Users participated in one dual and two individual interviews, while stakeholders were interviewed individually. Due to Covid-19 restrictions, eight of the eleven total interviews were conducted via online video calls.

Interview questions explored participants' motivations for joining Radar, their reflections on its practical use and data handling, perceived advantages and disadvantages, moral dilemmas encountered, responses to these dilemmas, and the need for ethical support in managing these challenges.

Data analysis

All interviews were first audio-recorded and then transcribed for in-depth analysis using an inductive thematic approach [21]. The initial stage focused on coding segments based directly on participants' perspectives. These codes were iteratively reviewed, combined, and refined to form broader categories, which ultimately represented three main ethical dimensions: values, moral dilemmas, and norms.

NVivo 12 software was used to organize the coding process, track emerging themes, and maintain analytic memos capturing insights, reflections, and team discussions. The first transcript was independently coded by three researchers (DB, EvB, BM), after which a joint discussion generated a preliminary thematic map. Subsequent transcripts were coded primarily by DB, with challenging sections discussed collaboratively to reach consensus. The resulting framework guided a second-level analysis, where patterns and relationships among codes were examined, leading to the identification of three overarching thematic categories that structured the study's findings. Any adjustments made during this phase were reviewed and agreed upon by the research team.

Research ethics

Participants were invited individually and provided with detailed information about the study's aims, data handling procedures, and confidentiality assurances, emphasizing that participation was entirely voluntary. This information was reiterated at the start of each interview. The unit commander was explicitly instructed not to influence participation, ensuring autonomy. All participants gave both written and oral informed consent. Data were anonymized and securely handled during collection, transfer, and storage.

The Medical Ethics Review Committee of VU University Medical Center determined that the study did not fall under the Dutch Medical Research Involving Humans Act (WMO) and waived formal approval. The study followed all relevant guidelines and regulations and is registered under number 2021.0363. Data supporting the study's findings are available from the corresponding author upon reasonable request.

Results and Discussion

Exploration of the ethical dimensions of PHM through participants' experiences with Radar highlighted several values and norms considered significant, some of which also raised ethical questions. From the thematic analysis, three interconnected categories emerged **(Figure 1):** (1) values, (2) moral dilemmas, and (3) external norms.

Values were both explicitly stated and implicitly reflected, spanning organizational concerns (the armed forces, commanders, and units), the PHM system itself (Radar), and individual user perspectives. Moral dilemmas were categorized into those directly experienced by participants and those anticipated or inferred. External norms, although less frequently mentioned, included adherence to legal frameworks for medical data collection, minimizing data collection to what is strictly necessary, and ensuring transparent, responsible data handling. Since these norms are rooted primarily in legislation—both military regulations [22] and the General Data Protection Regulation (GDPR) [23]—rather than participants' personal views, they are not discussed in depth. The findings also touch upon participants' perceptions of the need for ethical guidance and support in navigating PHM-related issues.

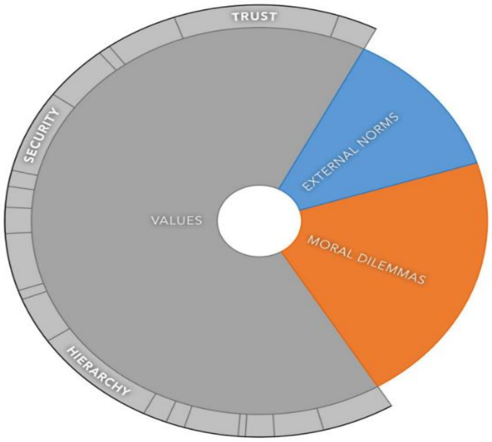

Figure 1. Illustrates the three main categories of ethical dimensions identified from the data, with the relative size of each section reflecting the number of coded references within that category.

Values

Analysis highlighted three primary values: (1) data security, (2) trust, and (3) hierarchy. In addition to these central values, several secondary values were identified that are closely connected to the main ones. A preliminary mapping of these core and related values is presented in **Figure 2.**

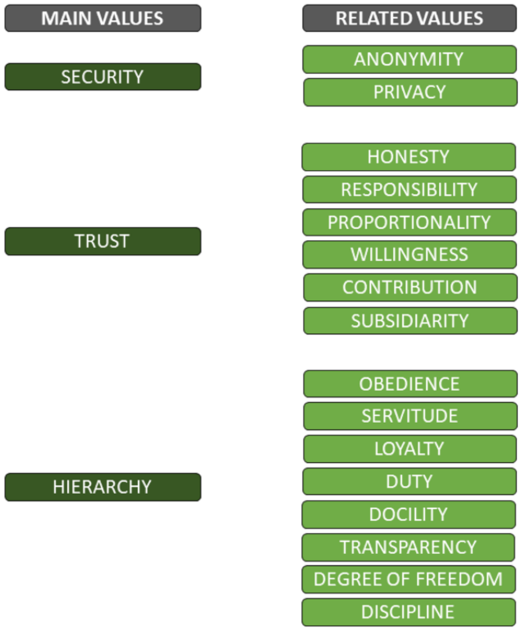

Figure 2. Overview of the identified main values and associated values

Values

Questions arose regarding the handling of data collected by Radar and the potential risks it may pose both to the armed forces as an organisation and to individual users. Consequently, security emerged as a key value for the respondents. Stakeholders view ensuring security as a shared responsibility of both the armed forces and the developers, aimed at safeguarding users, the organisation, and developers themselves from unauthorized or harmful access to the data. These concerns prompted both users and stakeholders to highlight the critical importance of this value. As noted by two participants, there is a shared understanding between users and stakeholders about the necessity of maintaining data security, which helps establish a standard.

Regarding information security, this is particularly pertinent given the target group—soldiers. It is essential to prevent sensitive soldier data from being exposed to foreign governments or other malicious parties. [stakeholder 6]

Additionally, I came to recognize an even more significant threat: the potential for data leaks. Such breaches could allow external or malicious actors to gain insight into the operational readiness of a unit. [user 4]

Trust

All responding users identified trust as a central value influencing their willingness to participate in Radar. Trust is shaped by users' experiences with their commander's leadership, the military hierarchy, and the potentially shared objectives of the organisation. It is also affected by Radar's possible outcomes and implications, including impacts on privacy. Users' ability to trust, and the extent of that trust, develops through socialisation. Respondents emphasized that context—such as the nature of the work, the safety of the environment, and whether tasks are mission-related or peacekeeping—also plays a critical role in shaping the level of trust required for participation.

One respondent highlighted the importance of leadership in establishing trust:

"When my commander gives instructions, I follow them almost without question. That trust has never been broken, so I can rely on it, which makes things much simpler. I can trust this part of the organisation completely." [user 3]

Trust is also influenced by confidence in the military hierarchy, clear communication from superiors, and leadership that makes participation appealing. These factors shape how users respond to orders or requests:

"During my time in the military, I temporarily committed my full attention and effort. This isn't a commercial choice—it's based on my confidence in the chain of command. Normally, if someone above me gives instructions, I trust them, unless something seems completely unreasonable. So participating in Radar didn't require much extra consideration." [user 3]

Respondents noted that their attitude toward privacy differs as soldiers compared to civilians. Within the military, they are more willing to compromise privacy, which is necessary for the organisation to function and shaped by operational context:

"I fully understand that some privacy must be sacrificed to ensure clarity about readiness." [user 1]

"I am more comfortable giving up some privacy than I would be outside the military. That's just how our organisation operates—information is needed to process requests and access resources. Participating in Radar wasn't a major leap for me." [user 2]

Trust is further reinforced by the organisation's goals and relationships within units. Respondents reported that advancing group or organisational interests often takes precedence over personal concerns. Trust in these higher objectives, along with confidence in colleagues, underpins this prioritisation and appears to stem from secondary socialisation:

"When necessary, the needs of the armed forces come before my own." [user 4]

"It's about setting aside personal concerns for the team's larger mission. I would do that. It's different for society at large, where I feel less inclined to intervene. Within the military, there's stronger camaraderie and a sense of unity." [user 3]

The degree of self-sacrifice depends on context and urgency. Respondents explained that during deployments, they are more willing to set aside personal interests, such as privacy, than during standard peacekeeping activities.

Trust is also reinforced by shared objectives regarding data security. Users recognised that keeping (medical) data secure benefits both the organisation and themselves, creating aligned interests:

"I trust that my medical information remains within the organisation, as this helps protect both the military and myself." [user 2]

Finally, respondents reflected on personal background and upbringing as influencing trust in both science and the military, which in turn motivated participation in Radar. Internalised values and norms acquired through primary socialisation serve as a foundation for the ability to trust:

"Having completed my university and PhD studies, I understand how science works, with room for discussion and careful evaluation. I trust professionals in government to make informed decisions more than random individuals. Additionally, growing up with a parent in a uniformed profession taught me to follow the guidance of public servants." [user 4]

Hierarchy

Hierarchy, a defining feature of military organisations, significantly influences participation in Radar. As highlighted by several respondents when discussing trust, hierarchy is implicitly linked to other values commonly associated with military culture. These intertwined values include obedience and docility. Users indicated that, both in general and in the context of Radar, they follow requests or orders from superiors without question:

"When a military superior makes a request, we usually just comply." [user 2]

This readiness to follow orders, combined with near-complete trust in leadership, connects to another key military value: loyalty. Respondents noted that enforcing rules or actions is often viewed as the most effective—or sometimes the only—way to achieve objectives. Soldiers are expected to carry out orders as part of their duty. Although participation in Radar was initially voluntary, respondents indicated that a broader, organisation-wide deployment would likely require mandatory compliance, potentially grounded in military legislation. However, they also emphasised that even if Radar were made compulsory, individual soldiers would probably choose not to use it if they were strongly opposed:

"It's not really up to the soldier whether to use Radar. In a proposed organisation-wide deployment, it would be mandatory. Still, if a soldier truly doesn't want to participate, they won't." [stakeholder 6]

Moral dilemmas and moral questions

No widely shared moral dilemmas, explicit or implicit, were identified. This section distinguishes between (a) dilemmas and questions actually experienced by respondents and (b) those presumed by them.

Experienced moral dilemmas and questions

Respondents described a tension between maintaining thoroughness and ensuring timeliness during the development of Radar. There was pressure to launch the app quickly to remain relevant. Regarding concerns about the validity of in-app questionnaires, one stakeholder noted:

"I understand that we need to compromise on the app's content to maintain momentum." [stakeholder 7]

Several respondents suggested involving experts earlier in the development and testing process. Implicitly, this reflects a dilemma between balancing accuracy and diligence with timeliness, as well as assuming responsibility for Radar's content:

"One could establish an advisory or expert group to decide on the content-related decisions for Radar." [stakeholder 7]

Other suggestions for future improvements focused on decision-making for organisation-wide deployment, particularly the need for prompt and decisive action:

"Decisions should be made quickly. We either proceed or we don't. The process has felt extremely prolonged." [stakeholder 3]

This highlights a dilemma between making careful, well-informed decisions and ensuring timely action. It also relates to uncertainties and moral doubts about the governance of Radar. Some stakeholders reported perceiving a lack of commitment at higher organisational levels to authorise Radar and take responsibility, questioning who decides participation and how outcomes will be used:

"How is governance structured? Who decides participation? Who determines what to do with the outcomes—a commander or a healthcare professional?" [stakeholder 7]

Another moral consideration concerns excluding civilian employees from Radar participation. Civilians cannot be mandated to use Radar, unlike soldiers. Respondents noted that this exclusion can make civilians feel undervalued, potentially affecting their mental wellbeing, employee-employer relationships, and overall job satisfaction.

Presumed moral dilemmas and questions

A potential moral dilemma identified by respondents concerns balancing individual and organisational interests, particularly the possible tension between privacy and security. Privacy protects the individual, while security safeguards the organisation. A stakeholder noted that these interests sometimes conflict and must be weighed against each other. In the context of Radar, privacy and security aligned, but this might not hold for other applications.

Some respondents expressed willingness to compromise personal privacy to support the protection of their unit during deployments, although this trade-off may differ during peacekeeping activities:

"During deployments, more can be expected, such as health monitoring, than during peacekeeping. Since it's a military organisation, I'm not too bothered by these expectations, but there are limits. Ultimately, personal interests take precedence over organisational goals in peacekeeping situations." [user 2]

This raises the moral question of what a military organisation can reasonably expect from its soldiers, given that individuals may be willing to forego certain personal interests to serve the organisation. This question becomes particularly relevant when considering core military values such as hierarchy, obedience, and loyalty.

Need for ethics support

To explore how ethics support could help address these experienced or presumed moral dilemmas related to Radar, stakeholders were asked whether such support would be valuable.

One respondent suggested that an ethics specialist could facilitate discussions to encourage stakeholders to think critically and identify potential moral issues. Another recommended forming a multidisciplinary group—including users, commanders, health professionals, legal advisors, and independent thinkers—to evaluate needs and possibilities for future health monitoring projects under various scenarios:

"I feel the need to think in terms of scenarios. Together with subject matter experts, we can develop scenarios and then examine the frame of reference—what is considered acceptable in each situation." [stakeholder 2]

Although most respondents did not explicitly demand ethics support, these suggestions indicate a recognized need for guidance in navigating moral dilemmas and questions related to personal health monitoring.

This study aims to examine the ethical dimensions of personal health monitoring (PHM) within the armed forces, with the goal of promoting its responsible use. We identified three central ethical dimensions of PHM: values, moral dilemmas, and external norms. Among the values, trust—particularly in leadership—emerged as the most critical, followed by hierarchy and security. These core values are closely linked to other identified values, including willingness, loyalty, and privacy. Our findings indicate that widely shared moral dilemmas, either explicit or implicit, were largely absent. The limited moral dilemmas that were reported primarily relate to Radar's content, ambiguities in governance surrounding its implementation and use, and the influence of contextual factors on users' willingness to prioritise organisational interests. Overall, stakeholders did not express a strong need for ethics support, though some highlighted the potential usefulness of involving an ethicist or a multidisciplinary advisory group. In the following discussion, we focus on the three main values identified to consider their implications for the future deployment of PHM in military contexts.

Both users and stakeholders emphasised the importance of data security. The ethical significance of safeguarding wearable technology, including PHM, is well-recognised in the literature [24, 25]. Unauthorized access to PHM data could pose personal risks to users, potentially outweighing the benefits of the technology. Within military organisations, data is often treated as a strategic asset [26]. PHM data, in particular, is valuable but also vulnerable, as it can reveal information about military readiness. Consequently, data breaches could present substantial risks to both soldiers and the organisation. Protecting sensitive information thus benefits both parties and requires robust measures. Ethical evaluation of PHM should therefore consider not only the impact of data protection on individual users (e.g., via a Data Protection Impact Assessment) but also its implications for the organisation. The benefits of PHM must be weighed against the potential harm arising from unauthorized access, which could compromise both personal safety and strategic advantage. In our study, users and stakeholders unanimously regarded security as essential. Failing to recognise and discuss the consequences of inadequate security could result in PHM usage where organisational interests override individual rights without proper deliberation. This underscores the importance of analysing data security from both user and organisational perspectives as part of ensuring morally responsible PHM use.

Data security extends beyond protecting digital information from unauthorized access, corruption, or theft; it is also closely intertwined with trust. Trust reflects users' confidence that the military will safeguard the data collected from them. PHM systems can enhance trust by allowing users to access, review, and control their data [27]. In the case of Radar, such features contributed to trust in the system. However, trust considerations may vary for future PHM applications or in different operational contexts, such as deployments. Even within a military setting where PHM participation could be mandatory, and personal health data may serve primarily organisational objectives, low trust can lead to non-use or deliberate manipulation of PHM data, with serious consequences for operational decision-making and mission outcomes. Providing transparent mechanisms for data control can strengthen trust, increase compliance, and enhance the reliability of PHM systems.

Furthermore, ongoing debates about security, privacy, and data ownership [28], along with the recognition of data as a potential human right [29], underscore the need for armed forces to carefully consider who owns soldiers' PHM data and who may access it under which circumstances.

Our study demonstrates that users place substantial trust in their commander, the organisation, and its intentions, which translates into a strong willingness to engage with PHM through Radar. This aligns with the cross-disciplinary conceptualisation of trust offered by Rousseau, Camerer, and Sitkin, who define trust as a psychological state in which one is willing to accept vulnerability based on positive expectations of another's intentions or behaviour [30]. The military environment, particularly during deployments, often involves high-risk situations where vulnerability, uncertainty, and interdependence are inherent. These conditions create a necessity for trust, as soldiers must rely on their commanders and colleagues to act competently, honorably, and with benevolent intentions [31]. Trust thus emerges as a central value, including in the context of PHM, where similar assumptions about intentions and competence apply.

Our findings indicate that trust is shaped by both interpersonal and organisational factors. Trust can be viewed as a fundamental need within military settings [32], yet it also carries potential risks. This trust may expose military users of PHM to latent vulnerabilities in balancing personal risks and benefits. For instance, respondents showed minimal concern about privacy—a primary ethical concern in the broader PHM literature [33, 34]. Notably, the reserve unit studied was not deployed to combat Covid-19, and therefore was not in a high-risk operational environment, which might otherwise require an even higher degree of trust. Despite this, respondents did not explicitly evaluate personal risks versus benefits when participating in Radar, prioritising organisational interests instead. Their participation decisions relied heavily on trust in their commander and the organisation. As Richards and Hartzog observe, "trust allows us to develop long-term, sustainable information relationships by sharing meaningful but often sensitive information and having sincere exchanges, with the confidence that what we share will be used for our benefit and not come back to haunt or harm us" [35]. Considering this, and the lack of privacy concerns in our study, it appears that respondents trusted that their data would be used responsibly for the benefit of both themselves and the organisation, without causing harm now or in the future. This foundational trust may also help explain why few moral dilemmas were experienced; the respondents did not question their commander or the organisation and therefore may have seen little need for critical reflection.

Interestingly, no widely shared moral dilemmas were reported by participants, which is notable given the broader debates surrounding employer-led health monitoring, particularly when it extends into personal domains [36]. Most respondents appeared to perceive monitoring Covid-19-related symptoms as necessary for evaluating military readiness amid the uncertainties of the pandemic. A high level of trust in leadership, combined with urgency to use Radar, likely contributed to the absence of reported dilemmas. Paradoxically, this strong trust may obscure certain ethical dimensions of PHM. Along with the limited number of experienced or presumed moral dilemmas, this explains why respondents expressed little demand for ethics support. We argue, however, that morally responsible PHM use requires ethical guidance to reveal and address these potentially hidden ethical issues.

Hierarchy, another key value in military contexts, is closely linked to trust. User responses suggest that the effectiveness of hierarchy—i.e., following commands or requests—depends on trust in leadership and the organisation. Although respondents did not explicitly discuss it, hierarchy, like trust, introduces potential vulnerability for service members, as they are expected to comply with orders and often cannot make independent decisions. While hierarchy serves an important operational purpose, namely clear command and control, acknowledging the vulnerabilities embedded in this structure is essential for ensuring morally responsible PHM deployment.

Previous studies have demonstrated that users are more likely to engage with PHM systems when they trust them [37]. Building on this, our research suggests that, in the armed forces, trust in leaders and the organisation—rather than trust in a specific PHM system—may be a particularly strong predictor of acceptance and use. Core military values, such as trust and hierarchy, also introduce vulnerabilities, especially in low-risk settings like peacekeeping operations. This vulnerability concerns, among other things, the ability of military personnel to weigh the risks and benefits of voluntary or mandatory interventions, including PHM, in a way that protects their personal interests while still supporting organisational objectives outside high-risk environments. It also relates to the principle of informed consent, which underpins all medical or research procedures and is grounded in the value of autonomy [38]. Scholars have questioned whether true informed consent is feasible in military contexts, given the constraints on autonomy imposed by hierarchical structures, command authority, training, and socialisation processes—all of which are intended to prioritise collective over individual needs [39, 40]. The combination of expressed trust, potential reductions in autonomy, and possibly hidden moral dilemmas in our study aligns with these concerns regarding genuine informed consent in the armed forces. While there may be some overlap, it remains uncertain to what extent these findings apply to PHM systems beyond active monitoring tools like Radar, which require users to respond to daily questionnaires. In passive monitoring systems, such as wearable devices, values like security, trust, and hierarchy could become even more critical, as users have less direct control over the data collected. Conversely, passive monitoring may also reduce users' awareness that they are being monitored, potentially decreasing the prominence of trust as a concern.

Within the military, hierarchy and the necessary trust in leaders, orders, and the organisation extend beyond high-risk contexts. This creates a moral obligation to manage trust and hierarchy responsibly, particularly in low-risk environments, and to implement safeguards that protect this potentially vulnerable population [40-42]. Such responsibilities include carefully considering the role of ethics support when implementing PHM systems, particularly given ongoing risks of large-scale data breaches, misuse, and privacy violations [43]. Although not the focus of this article, external norms—such as laws, regulations, and organisational policies—remain crucial for ensuring the safe, accurate, and privacy-compliant use of PHM [44]. Within the European Union, frameworks like the General Data Protection Regulation, the Medical Device Regulation, national legislation, and specific military regulations must collectively safeguard users from unsafe, inaccurate, or privacy-infringing PHM practices.

Overall, this study contributes to raising awareness of the ethical dimensions of PHM and provides insights for identifying and addressing key ethical dilemmas in future systems. Additionally, these findings complement ongoing discussions in military medical ethics concerning the responsible use of technical medical knowledge for military purposes [45].

Strengths and limitations

A major strength of this study is that, to our knowledge, it is among the first to examine the values, norms, and moral dilemmas related to PHM within the armed forces. Rather than relying on a top-down expert perspective, it draws on empirical insights from multiple groups, including both users and various stakeholders, grounded in their actual experiences. This approach complements existing research on the ethical considerations of PHM in civilian healthcare and contributes to the field of military medical ethics. The results may inform future research, guide the development of normative frameworks, and support policymakers in their decision-making.

Several limitations should be acknowledged. The findings from this national reserve unit may not be representative of the wider armed forces, as this unit has distinct demographics, including a higher median age and education level. Participation in Radar was voluntary, which may have fostered an initially positive attitude toward PHM and influenced study results. Moreover, the low response rate among users could have affected the identified composition and hierarchy of values. The preliminary overview of values presented in **Figure 2** is not a comprehensive, systematic classification; the relationships between these values and their implications for responsible PHM use require further investigation.

The low response rate may reflect several factors, including high personnel turnover, infrequent use of work emails, inability to participate due to regular civilian work duties, or lack of perceived urgency. Privacy regulations restricted recruitment to work email communication, and members who did not use Radar were not included, potentially omitting relevant perspectives on the ethical dimensions of PHM. Additionally, interviews were conducted several months after participants had stopped using Radar, during a period when the Covid-19 situation was evolving rapidly (e.g., fluctuating incidence rates, initiation of national vaccination campaigns). This timing may have influenced respondents' recollections, their assessment of important values, and their perception of moral dilemmas while actively using Radar. To mitigate potential recall bias, interviewers provided a brief overview comparing the Covid-19 situation at the time of Radar use with the current situation at the start of each interview to refresh participants' memories.

Conclusion

This study explored the experiences and perspectives of users and stakeholders regarding the ethical dimensions of PHM in the Netherlands Armed Forces. Findings illuminate the range of values perceived as important by different stakeholders and indicate that respondents generally experienced few or weak moral dilemmas. Nevertheless, some participants suggested the potential utility of ethics support. Key values identified include data security, trust, and hierarchy. Trust in PHM is closely related to leadership, shared organisational goals, the consequences of PHM, and socialisation processes. These values, however, may also create vulnerabilities for military users when personal and organisational interests are misaligned, with trust potentially limiting critical deliberation on the ethical aspects of PHM. The context in which PHM is developed and implemented plays a significant role in user acceptance and compliance.

The findings underscore the ethical responsibility of the armed forces to pay careful attention to PHM's moral dimensions. Ethics support can help uncover and address potentially hidden moral dilemmas, thereby supporting responsible PHM use. Future research could further explore service members' vulnerabilities in relation to trust and hierarchy, investigate concealed ethical issues in the development, implementation, and use of PHM, and examine different approaches to ethics support. Considering distinctions between active and passive monitoring systems, as well as variations in context—such as active military duty versus reserve units, peacekeeping versus deployment, and prevention versus treatment of illness—may reveal additional values and moral dilemmas relevant to PHM use.

Acknowledgments: None

Conflict of Interest: None

Financial Support: None

Ethics Statement: The Medical Ethics Review Committee of VU University Medical Center confirmed that the Dutch Medical Research Involving Humans Act (WMO) did not apply. The need for approval was waived by the Medical Ethics Review Committee of VU University Medical Center. This study is registered at the Medical Ethics Review Committee of VU University Medical Center under the number 2021.0363. All experiments were performed in accordance with relevant guidelines and regulations. All participants provided written and oral informed consent to participate in the study.

References

1. Grandview Research. mHealth Market Size, Share & Trends Analysis Report, 2022–2030. 2022. Available from: https://www.grandviewresearch.com/industry-analysis/mhealth-market
2. Guk K, Han G, Lim J, Jeong K, Kang T, Lim EK, et al. Evolution of wearable devices with real-time disease monitoring for personalized healthcare. Nanomaterials (Basel). 2019;9(6):1013.
3. Haghi M, Thurow K, Stoll R. Wearable devices in medical internet of things: scientific research and commercially available devices. Healthc Inform Res. 2017;23(1):4–15.
4. Van der Vaart R, Van Deursen L, Standaar L, Wouters M, Suijkerbuijk A, Van Tuyl L, et al. E-healthmonitor 2021: stand van zaken digitale zorg. Bilthoven: Rijksinstituut voor Volksgezondheid en Milieu; 2022.
5. Mittelstadt B. Personal health monitoring. 2013.
6. Suh MK, Chen CA, Woodbridge J, Tu MK, Kim JI, Nahapetian A, et al. A remote patient monitoring system for congestive heart failure. J Med Syst. 2011;35(5):1165–79.
7. European Centre for Disease Prevention and Control. Mobile applications in support of contact tracing for COVID-19 – a guidance for EU/EEA Member States. Stockholm: ECDC; 2020.
8. Chae SH, Kim Y, Lee KS, Park HS. Development and clinical evaluation of a web-based upper limb home rehabilitation system using a smartwatch and machine learning model for chronic stroke survivors: prospective comparative study. JMIR Mhealth Uhealth. 2020;8(7):e15196.
9. Hall K, Oesterle S, Watkowski L, Liebel S. A literature review on the risks and potentials of tracking and monitoring eHealth technologies in the context of occupational health management. Wirtschaftsinformatik 2022 Proceedings.
10. Friedl KE. Military applications of soldier physiological monitoring. J Sci Med Sport. 2018;21(11):1147–53.
11. Adler AB, Gunia BC, Bliese PD, Kim PY, LoPresti ML. Using actigraphy feedback to improve sleep in soldiers: an exploratory trial. Sleep Health. 2017;3(2):126–31.
12. Bustos D, Guedes JC, Vaz MP, Pombo E, Fernandes RJ, Costa JT, et al. Non-invasive physiological monitoring for physical exertion and fatigue assessment in military personnel: a systematic review. Int J Environ Res Public Health. 2021;18(16):8818.
13. Buller MJ, Delves SK, Fogarty AL, Veenstra BJ. On the real-time prevention and monitoring of exertional heat illness in military personnel. J Sci Med Sport. 2021;24(10):975–81.
14. Nordgren A. Personal health monitoring: ethical considerations for stakeholders. J Inform Commun Ethics Soc. 2013;11(3):156–73.
15. Mittelstadt B, Fairweather B, Shaw M, McBride N. The ethical implications of personal health monitoring. Int J Technoethics. 2014;5(2):37–60.
16. Bowes A, Dawson A, Bell D. Ethical implications of lifestyle monitoring data in ageing research. Inf Commun Soc. 2012;15(1):5–22.
17. Gilmartin C, Arbe-Barnes EH, Diamond M, Fretwell S, McGivern E, Vlazaki M, et al. Varsity medical ethics debate 2018: constant health monitoring the advance of technology into healthcare. Philos Ethics Humanit Med. 2018;13(1):12.
18. Leikas J, Kulju M. Ethical consideration of home monitoring technology: a qualitative focus group study. Gerontechnology. 2018;17:38–47.
19. Mittelstadt B. An ethical analysis of personal health monitoring in the UK. ORBIT J. 2018;1(1).
20. Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol. 2006;3(2):77–101.
21. Rijksinstituut voor Volksgezondheid en Milieu. De ziekte COVID-19. 2020. Available from: https://www.rivm.nl/coronavirus-covid-19/ziekte
22. Wet ambtenaren defensie. 2021. Available from: https://wetten.overheid.nl/BWBR0001952/2021-01-01
23. General Data Protection Regulation. 2016. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
24. Habibipour A, Padyab A, Ståhlbröst A. Social, ethical and ecological issues in wearable technologies. AMCIS 2019 Proceedings; Cancun. 2019.
25. Anaya L, Alsadoon A, Costadopoulos N, Chua P. Ethical implications of user perceptions of wearable devices. Sci Eng Ethics. 2018;24(1):1–28.
26. Department of Defense. DoD Data Strategy 2020. Department of Defense; 2020.
27. Mittelstadt B, Fairweather B, McBride N, Shaw M. Privacy, risk and personal health monitoring. In:

ETHICOMP 2013 Conference Proceedings; ETHICOMP 2013, Kolding, Denmark.

28. Hummel P, Braun M, Dabrock P. Own data? Ethical reflections on data ownership. Philos Technol. 2021;34(3):545–72.
29. United Nations. A human rights-based approach to data. 2018.
30. Rousseau DM, Sitkin SB, Burt RS, Camerer C. Not so different after all: a cross-discipline view of trust. Acad Manage Rev. 1998;23(3):393–404.
31. Adams B, Webb R. Trust in small military teams. 2002.
32. Collins JJ, Jacobs TO. Trust in the profession of arms. In: Snider DM, Watkins GL, editors. The future of the army profession. Boston: McGraw-Hill Primis Custom Publishing; 2002. p. 39–58.
33. Dinh-Le C, Chuang R, Chokshi S, Mann D. Wearable health technology and electronic health record integration: scoping review and future directions. JMIR Mhealth Uhealth. 2019;7(9):e12861.
34. Cilliers L. Wearable devices in healthcare: privacy and information security issues. Health Inf Manag. 2020;49(2–3):150–6.
35. Richards N, Hartzog W. Privacy’s trust gap: a review. Yale Law J. 2017;126(4):1180–224.
36. Maltseva Reiby K. Wearables in the workplace: the brave new world of employee engagement. Bus Horiz. 2020;63(3):357–66.
37. McLean A. Ethical frontiers of ICT and older users: cultural, pragmatic and ethical issues. Ethics Inf Technol. 2011;13(4):313–26.
38. Beauchamp T. Autonomy and consent. In: Miller F, Wertheimer A, editors. The ethics of consent: theory and practice. Oxford: Oxford University Press; 2009. p. 55–78.
39. Latheef S, Henschke A. Can a soldier say no to an enhancing intervention? Philosophies. 2020;5(3):13.
40. Coleman N. The impact of the duty to obey orders in relation to medical care in the military. In: Messelken D, Winkler D, editors. Ethics of medical innovation, experimentation, and enhancement in military and humanitarian contexts. Cham: Springer International Publishing; 2020. p. 37–52.
41. Parasidis E. The military biomedical complex: are service members a vulnerable population? Hous J Health L Pol’y. 2019;16:1–45.
42. Shivayogi P. Vulnerable population and methods for their safeguard. Perspect Clin Res. 2013;4(1):53–7.
43. Pipikaite A, Bueermann G, Joshi A, Jurgens J. Global cybersecurity outlook 2022. Geneva: World Economic Forum; 2022.
44. Majmudar MD, Colucci LA, Landman AB. The quantified patient of the future: opportunities and challenges. Healthc (Amst). 2015;3(3):153–6.
45. Bricknell M, Story R. An overview to military medical ethics. J Mil Veterans Health. 2022;30(2):7–16.