International Journal for Quality Research 18(1) 43–64
ISSN 1800-6450

María Belén Ortiz[1]
Stanislav Karapetrovic

Article info:
Received 10.09.2022.
Accepted 15.07.2023.

UDC – 006.013
DOI – 10.24874/IJQR18.01-04

VALIDATING IoT-RELATED ISO 10001 HAND HYGIENE PRIVACY CODES IN HEALTHCARE

Abstract: *Six Healthcare Workers' Hand Hygiene Privacy Codes (HW-HH-PCs), addressing data collected through an automated HH Monitoring Technology (HHMT), are validated. These HW-HH-PCs illustrate integrative augmentation with ISO 10001:2018 customer satisfaction and ISO/IEC 27701:2019 privacy management standards. A focus group of infection preventionists, managers and technology specialists from a Canadian hospital was conducted to verify the HW-HH-PCs' feasibility. An electronic survey and personal interviews with HWs from the hospital were then performed to evaluate the perceived importance of the three feasible and additional HW-HH-PCs. HWs recognized the feasible codes as important and reported feeling more comfortable with the automated HHMT if they were to be established. This paper may be the first to present empirical data about the feasibility and perceived importance of privacy-related codes that follow ISO 10001 and ISO/IEC 27701 guidelines.*

Keywords: *customer satisfaction, privacy, internet of things, healthcare, standards, integrated management systems*

1. Introduction

Healthcare organizations monitor adherence to Hand Hygiene (HH) procedures as HH is critical for preventing hospital-acquired infections (WHO, 2009; Conway, 2016; Meng et al., 2019). Automated Hand Hygiene Monitoring Technologies (HHMTs) are tools for tracking HH compliance (Pong et al., 2018; Boyce et al., 2019; Iversen et al., 2020). Here, qualified reviewers observing HH compliance directly (Boyce, 2008; Sax et al., 2009; Tarantini et al., 2019) are substituted with sensors (McGuckin and Govednink, 2015). Advantages of such HHMTs include producing real-time information about HH behaviour (Benudis et al., 2019) through a monitoring process less affected by biases (Ellingson et al., 2011; Conway, 2016).

However, as with other technologies based on the Internet of Things (IoT) deployed in healthcare (Lowens et al., 2017; Boonstra et al., 2018; Pal et al., 2018; Auepanwiriyakul et al., 2020), users of IoT-based HHMTs have expressed concerns related to the collection and deployment of data gathered through these technologies (Boscart et al., 2008, Ellingson et al., 2011; Dyson and Madeo, 2017; Tarantini et al., 2019; Blomgren et al., 2021). Authors such as Birchley et al. (2017), Boonstra et al. (2018), Alraja et al. (2019) and Grant et al. (2019) have proposed strategies to mitigate privacy-

[1] Corresponding author: María Belén Ortiz
Email: mortizg@utec.edu.pe

related users' worries about sensor-based technologies applied in healthcare. These strategies include giving users the option to decide what data they are willing to share (Birchley et al., 2017) and when the technology should stop monitoring them (Grant et al., 2019), as well as offering an explicit description of the purposes for data collection as part of the consent process (Boonstra et al., 2018). The provision of guarantees by IoT suppliers is another related strategy (Alraja et al., 2019).

According to the ISO 10001 standard (ISO, 2018b), a guarantee and the corresponding requirements (respectively called "*a promise*" and *"provisions"* in ISO 10001: 2018) are the components of a Customer Satisfaction (CS) code. Ortiz and Karapetrovic (2021 and 2022) demonstrated six ISO 10001 CS codes that healthcare organizations could offer to the Healthcare Workers (HWs) who use electronic devices for HH monitoring. These codes pertain to a healthcare organization's collection and usage of the automated HHMT-gathered Personally Identifiable Information (PII). To prepare them, Ortiz and Karapetrovic (2021 and 2022) applied ISO 10001 guidelines in combination with selected ISO/IEC 27701 provisions for privacy management.

This paper presents the findings from a focus group conducted with hospital managers, infection preventionists and technology specialists to verify the feasibility of the six CS codes and related resources proposed in Ortiz and Karapetrovic (2021 and 2022). Hospital managers are the *"PII controllers"* as they decide the purposes for, and the manner of, collecting the PII related to HH compliance (ISO/IEC 29100, clause 2.10). Infection preventionists and technology specialists are examples of *"PII processors"* since they process the PII related to HH compliance *"on behalf of and in accordance with the instructions"* of the hospital managers (ISO/IEC 29100, clause 2.12). The focus group took place at a Canadian hospital that had implemented an HHMT in a pilot project. The results of an electronic survey and online interviews with HWs from the same hospital to evaluate how important these codes were to them are also reported.

A literature review regarding the characteristics and benefits of CS guarantees, examples of such guarantees for external and internal customers in healthcare, as well as integrative augmentation of CS and privacy management systems (MSs), is presented first. The methodology followed to verify the feasibility of the six privacy-related codes proposed in Ortiz and Karapetrovic (2021 and 2022) and to evaluate their importance to HWs is shown next. Focus group, survey and interview results are subsequently discussed. Finally, conclusions concerning the relevance of the validated codes for healthcare organizations and integrative augmentation are examined.

2. Literature Review

A CS "guarantee" consists of a service-related promise made by an organization to its customers and a description of the actions the organization will take if this promise is not fulfilled (Hart et al., 1992; Kashyap, 2001; Hogreve and Gremler, 2009). CS guarantees must address characteristics of the service relevant to customers (Hart, 1993; Fabien, 2005; Berman and Mathur, 2014). When a service provider implements a CS guarantee, customers may perceive the utilization of the service as less risky (Wirtz et al., 2000; Boshoff, 2002; Lee and Khan, 2012; Berry, 2019) and trust the service more (Berry, 2019).

CS guarantees implemented in healthcare deal with issues related to waiting times (Raffio, 1992; Kumar et al., 1997; Guo et al., 2004; Franklin, 2018), service billing (Raffio, 1992), response times (Raffio, 1992, Thomassen et al., 2014) and service discounts (Raffio, 1992). Other healthcare-related guarantees address the participation of patients in treatment decisions (Thomassen et al., 2014), provision of information to patients about the healthcare organization (Thomassen et al., 2014) and the care plan (Khan, 2016; Khan and Karapetrovic, 2013 and 2015), as well as respectful treatment of patients (Thomassen et al., 2014), including staff's introduction to them (Khan, 2016; Khan and Karapetrovic, 2013 and 2015).

CS guarantees that address the handling of customer information in healthcare are scarce. Thomassen et al. (2014) presented a promise made by healthcare organizations working together to provide an *"integrated stroke service."* According to this promise, each organization will share a patient's relevant information with the organization following up on their care process (Thomassen et al., 2014). Courneya et al. (2013) introduced a guarantee provided by an online clinic that patients can invoke when they are dissatisfied with any service feature. This guarantee is for *"refund[ing] [the] cost"* of the service in case of customer dissatisfaction (Virtuwell, 2022a). Although the guarantee does not seem to be focused on a single service feature only, the online clinic's webpage also states: *"...your information is protected at every step…"* (Virtuwell, 2022b), thereby identifying privacy as one such specific feature.

All healthcare-related CS guarantees found in the literature are aimed at patients (e.g., Thomassen et al., 2014; Khan and Karapetrovic, 2013 and 2015; Khan, 2016), except those introduced in Ortiz and Karapetrovic (2021 and 2022), who proposed six CS guarantees, labelled as *"Healthcare Workers' Hand Hygiene Privacy Codes"* (HW-HH-PCs), concerning the privacy of the information collected through an automated HHMT. These six codes are directed at HWs, who are regarded as internal customers in healthcare (Bellou, 2010; Manolitzas et al., 2014), and to whom a healthcare organization provides a service, which includes the automated HHMT and the information related to it (ISO/IEC 20000-1, clause 3.2.18; Ortiz and Karapetrovic, 2020).

Two HW-HH-PCs (i.e., HW-HH-PCs '1' and '2') were presented in Ortiz and Karapetrovic (2021). Ortiz and Karapetrovic (2022) introduced four other HW-HH-PCs (i.e., HW-HH-PCs 'A', 'B', 'C' and 'D'). Letters were used to label Ortiz and Karapetrovic (2022)'s codes to avoid repeating the numbered labels already deployed in Ortiz and Karapetrovic (2021). HW-HH-PCs-1, -A and -B established that the healthcare organization would only:

- use the PII collected through the automated HHMT for the purposes communicated to the HWs ('1'),
- provide access to this PII to people in the roles conveyed to the HWs ('A'), and
- collect the PII reported to the HWs ('B').

HW-HH-PC-2 stated that the healthcare organization would share the automated HHMT-processed HH compliance rates exclusively with the HW to whom these rates pertain. HW-HH-PC-C indicated that the HW would be able to choose whether or not to display their name on the reports produced by the automated HHMT. Lastly, HW-HH-PC-D stated that the healthcare organization would not use the HHMT-collected HH compliance rates for disciplinary action.

Those six codes followed ISO 10001, which is an "augmenting" standard, as it focuses on a specific part of a quality Management System (MS) and helps develop additional processes to improve this MS (Karapetrovic, 2005). ISO/IEC 27701 is also an augmenting standard since it enhances an ISO/IEC 27001 information security MS by providing guidelines for privacy management (ISO, 2019). Integrative augmentation of ISO 10001 and ISO/IEC 27701 was first presented in Ortiz and Karapetrovic (2020, 2021 and 2022). However, these articles only investigated such integrative augmentation conceptually, without presenting an empirical validation.

3. Research Methodology

This paper reports on a model validation component of a two-stage study. The first stage focused on developing a model for the augmentation of CS systems with privacy-related subsystems to manage users' satisfaction with IoT-based HHMTs. The second stage, whose results are partially presented here, concentrates on validating this model in a Canadian hospital, hereinafter, the "Case Study Hospital" (CSH). The CSH conducted a study in 2018 at one of its units to pilot a sensor-based HHMT for the purposes of evaluating its acceptability and feasibility. The HMMT had not been deployed in other hospital units at the moment of our study.

Three specific elements of the second stage are specifically examined:

- validation of the feasibility of the six HW-HH-PCs presented in Ortiz & Karapetrovic (2021 and 2022) with PII controllers and PII processors,
- verification of the importance for HWs of the HW-HH-PCs deemed feasible by PII controllers and PII processors,
- validation of the feasibility and suitability of other elements of the ISO 10001 HW-HH-PC system described in Ortiz & Karapetrovic (2020, 2021 and 2022) with PII controllers, PII processors and HWs.

A focus group was conducted first to verify the feasibility of six HW-HH-PCs (ISO 10001, 6.3). Some focus group participants represented the PII controllers (e.g., hospital managers) and others the PII processors (e.g., infection preventionists). The focus group participants had taken part in planning the pilot study conducted in 2018, and, therefore, understood the technology and how the CSH had been planning to manage it. An interview guide was used for a one-hour discussion, which involved six participants. Three HW-HH-PCs were considered feasible. Additional questions regarding feasible HW-HH-PCs were asked, including inquiries concerning the required resources, as well as the potential methods to inform PII processors and principals about these codes and to provide feedback on them.

Secondly, HW-HH-PCs' importance for HWs was verified through the following two steps:

1) An electronic survey with 18 questions was sent to 230 CSH's HWs who could potentially use the automated HHMT (ISO 10001, 6.3). These HWs represented PII principals as they *"provide their PII* [i.e., HH compliance rates and other PII collected through the automated HHMT] *for processing to PII controllers* [e.g., hospital managers] *and PII processors* [e.g., infection preventionists]…" (ISO/IEC 29100, clause 4.2.1). Unlike the focus group participants, not all HWs had been involved in the pilot study and, therefore, were familiar with HHMTs. For this reason, an animated video, explaining how automated HHMTs work (e.g., see Boscart et al., 2008; Levchenko et al., 2014; Benudis et al., 2019) and providing context for the questions about information security, privacy and promises, was shared with the HWs at the beginning of the survey. Nine completed surveys were received after three rounds of sending the recruitment email. Questions 17 and 18 were answered by eight participants only.
2) Online interviews using a related guide were conducted with two HWs who could potentially use the automated HHMT (ISO 10001, 6.3). The animated video from the survey was shown at the beginning of the interview. The questions concerned the importance of the four HW-HH-PCs included in the survey and an additional HW-HH-PC

proposed by a focus group participant. They also related to particular HW-HH-PCs elements, namely the adequacy of code nonfulfillment actions (ISO 10001, 6.4.e), the clarity of the HW-HH-PC scope (ISO 10001, 6.4.a) and key terms (ISO 10001, 6.4.c). In addition, interview participants were asked how HWs using the automated HHMT should be informed about the HW-HH-PCs and how these users could provide feedback on these codes.

4. Results

4.1. Verifying the feasibility of HW-HH-PCs with PII controllers and processors

Table 1 presents the focus group discussion results regarding the feasibility of the codes. For instance, the participants mentioned a *"learning plan"* when discussing promises 'C' and 'D', so that, in cases of recurrent non-compliance, the HW would develop such a plan with support of a member of the HH compliance team (e.g., an infection preventionist). The *"learning plan"* would include actions that the HW would take to improve their HH compliance rates and the corresponding deadline for each activity.

The "*wearable device*" mentioned by focus group participants refers to an electronic device worn by HWs, which records the hand sanitizer dispenser activation (i.e., an HH action) and the entry to, or exit from, the patients' room (i.e., an HH opportunity) (Dyson and Madeo, 2017; Pong et al., 2018; Boyce et al., 2019).

According to the participants, the promises of codes '2', 'C', and 'D' were unfeasible since the CSH might need to link the device to the HW in case of serious non-compliance. This linkage would allow the CSH to identify device-related technical problems and establish a *"learning plan"* or other corrective actions if required.

Table 1. Feasibility of the proposed CS codes according to the focus group participants

HW-HH-PC Label	Feasible?	Participant	Reasons
1	Yes	Four	• Considered these promises feasible since the HH compliance team had already prepared consent forms identifying what information the team was collecting. Moreover, there was an agreement on who would have access to the data if the wearable device were linked with the HW. • Also pointed out that "*the only challenge would be unforeseen circumstances or a breach,* [but those] *might even be addressed in the consent forms*".
A	Yes	Three	Stated that the *"bedrock of any research study is how you handle PII"*.
B	Yes	Two	Reported being initially unsure about the CSH's ability to fulfill promise A when the HHMT is fully implemented, as opposed to the pilot project. However, they pointed out that "[after rereading the promise, they realized that as long as HH compliance team members] *or management are identified* [on the consent form (because HH monitoring is a part of their job), the CSH] *would be covered* [against HWs' complaints] *and not in violation of the code".*
2	No	Three	Pointed out that the CSH could not make this promise as it would prevent the HH compliance team from tracking down the causes of non-compliances individually.

HW-HH-PC Label	Feasible?	Participant	Reasons
		Five	• Indicated that “[in cases of] *severe non-compliance* [or suspicion that the wearable device] *is not working* [correctly, the HH compliance team would need to] *link* [it] *with the HW.* [Therefore, they would also have] *a way to check* [this user’s] *compliance rates*”. • Said that the “[HH compliance team] *would have to go outside of the code if they noticed something weird* [with the data collected to verify that the problem was not related to the wearable device]”.
		Four	Mentioned that “[the CSH could not guarantee this promise because the HH compliance team] *would have to talk with managers about a* [potential] *disciplinary action and break the code if* [they] *noticed low* [HH] *compliance rates”.*
C	No	Five	• Mentioned that “[the] *reports* [produced by the HHMT used in the pilot project] *only show the* [wearable device] *number by default.* [Therefore,] *the default* [for this HHMT’s reports] *is anonymous unless someone wants* [to show] their names”. • Also indicated that “[they did] *not see an issue with* [this promise] *if* [the feature] *is a part of the technology and* [users] *want to deanonymize themselves”.*
		Two	Pointed out that this promise could lead to confusion since it should be clear that it is only about not displaying users’ names and not for delinking them from the wearable device (i.e., the HH compliance team would still know who is who).
		Four	
		One	Reiterated the “[importance of knowing to whom the information pertains in order to] *develop* a *learning plan* [if needed]. Additionally, “*if there is a problem with the* technology, [technology specialists] *can fix it”.*
D	No	Two	Pointed out that “[although] *it would be nice to say* [that the CSH would not use the data for disciplinary action from a philosophical perspective, there are] *some circumstances* [in which they] *may need to* [do it]”.
		Four	• Said that “if [the compliance group observes] *low* [HH] *compliance* [rates] *from the same HW, there are ethical implications about not doing something about it”.* • Also indicated that “[they] *would first troubleshoot* [to ensure a technological problem did not cause the low HH compliance rates. Then, they] *would work with the HW on a learning plan to improve* [their compliance] *rates. If the problem persists,* [the HH compliance team] *would have to involve the manager* [to decide] *what to do next”.*
		One	Mentioned that, “[although the primary purpose of the data collected through the IoT-based HHMT is not] *disciplinary action,* [this data] *would be incorporated into the learning plan. If the* [behavioural] *problem continues,* [it] *would have to be escalate(d) it to management* [to address it]”.

As part of the discussion on HW-HH-PCs-1, -A and -B, a participant suggested an additional feasible code concerning the PII gathered through the automated HHMT. According to this participant, the CSH could promise to collect only the minimum amount of PII necessary for the study. Based on this suggestion, a new code was developed.

The new code elements presented in Table 2 illustrate the augmentation of the ISO 10001 code system with the ISO/IEC 27701 and ISO/IEC 29100 privacy subsystems. The tabular approach used in Ortiz and Karapetrovic (2021 and 2022) was applied to map the ISO/IEC 27701 and ISO/IEC 29100 guidelines to each of the five elements of the new code (i.e., "promise," "action," "terms," and "feedback"). The promise is in line with sections 7.4.1 of ISO 27701: 2019 and 5.4 of ISO 29100: 2011. Both clauses indicate that organizations should limit the collection of PII to what is "necessary" for established purposes. Clause 7.4.1 of ISO/IEC 27701 additionally states that the organization should limit PII collection to the *"minimum"* that is *"adequate"* and *"relevant"* for such purposes.

Processing only the *"necessary"* information implies that the CSH should not collect more information than they need to fulfill the purpose of monitoring HH compliance (Information Commissioner's Office, 2021). For example, information about the time of entry to, or exit from, an area different from the patient's room may not be necessary. Collecting only *"relevant"* PII means that *"a rational link"* must exist to the specified purpose for collecting PII (Cook, 2020; Information Commissioner's Office, 2021). In the context of automated HHMT, gathering information, for instance, on HW's age, would not be relevant for tracking HH compliance. Collecting the minimum PII that is *"adequate"* means that the CSH should gather *"sufficient* [PII] *to properly fulfill"* the specified purpose (Information Commissioner's Office, 2021). For example, the automated HHMT needs to collect information about entry to, or exit from, patient rooms as "*prox*[ies]" of HH opportunities (Dyson and Madeo, 2017; Boyce et al., 2019).

Table 2. ISO/IEC 27701 & ISO/IEC 29100 supporting the new HW-HH-PC's elements

Element name	Elements of the HW-HH-PC proposed in focus group	ISO/IEC 27701	ISO/IEC 29100	ISO 10001
Promise	The hospital will *"limit the collection of personally identifiable information* [through the automated hand hygiene monitoring system] to [the minimum that] *is adequate, relevant and necessary* [for the] *purposes* [that are both identified on the consent form and communicated to the healthcare worker]" (ISO/IEC 27701, 7.4.1)	7.4.1	5.4	6.4.b
Actions	Otherwise, the hospital will record information about the incident and initiate a review to determine the *"measures* [...] *to be taken"*(ISO/IEC 27701, 6.13.1.5)	6.13.1.5		6.4.e
Scope and limitations	This code applies to any personally identifiable information (PII) collected through the automated hand hygiene monitoring system.			6.4.a
Terms	*"PII is any information that (a) can be used to identify the* [healthcare worker] *to whom such information relates, or (b) is or might be directly or indirectly linked to the* [healthcare worker]" (ISO/IEC 29100, 2.9)		2.9	6.4.c
Feedback	Healthcare workers can provide feedback about this code and its use by sending an email.			6.4.d

The rest of the new HW-HH-PC's elements are the same as those of HW-HH-PC-A and -B presented in Ortiz & Karapetrovic (2022). Thus, for instance, the "actions" element follows the guidance for *"information security incidents response"* provided in ISO/IEC 27701 (clause 6.13.1.5). The importance of this additional HW-HH-PC (labelled as 'E') was assessed through online interviews with HWs. The related results are shown in section 4.3.

Since HW-HH-PC-1, -A and -B were identified as feasible, an additional question regarding these codes was asked in the focus group, namely whether the actions proposed if these promises are not fulfilled (ISO 10001, 6.4.e) were also feasible. Participants stated that the actions were viable as they align with many of their current review processes when there is a breach concerning, for example, information security related to other technologies. As a result, they obtain outcomes they act upon based on consensus.

When asked how the CS codes could be conveyed to PII processors (ISO 10001, 6.7), a participant mentioned that they should be *"definitely"* communicated in staff meetings. Other participants noted that these codes could be shared with PII processors through a "weekly newsletter", "quality boards," and quality meetings held at the start of work shifts. Participants also indicated that they did not think HW-HH-PCs should be included in PII processors' contractual agreements as Ortiz & Karapetrovic (2020) proposed.

4.2. Surveying PII principals with respect to the HW-HH-PCs

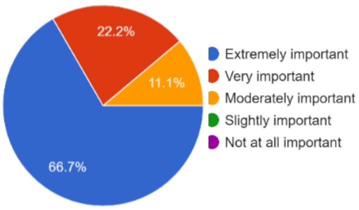
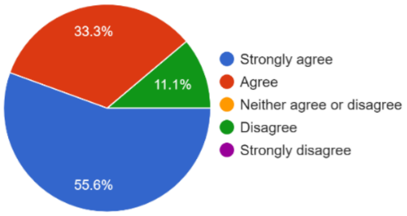
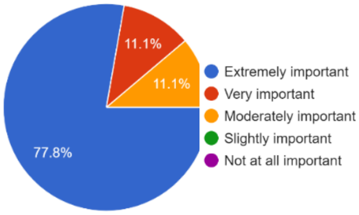
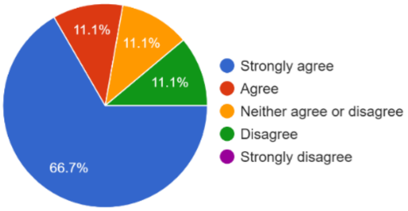
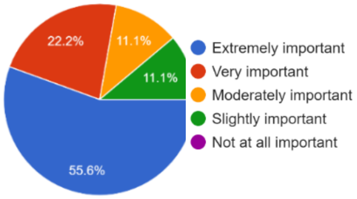
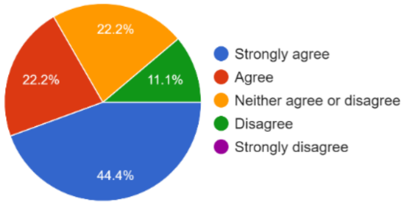
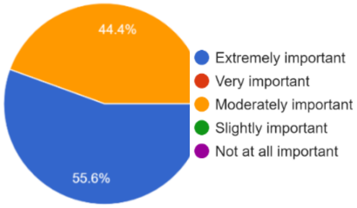
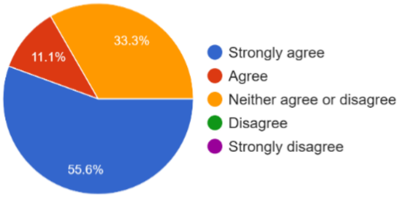
The objective of Questions 1 to 5 in the survey was to learn whether HWs at the CSH shared certain privacy-related concerns identified in the literature. This was done to verify if the issues that the proposed codes address are present at this particular CSH, in alignment with clauses 6.2 and 6.3 of ISO 10001. The issues verified through these questions are connected with both the CS codes, on the one hand, and privacy, on the other, and in turn, with integrative augmentation of the ISO 10001 code system by its ISO/IEC 27701 privacy subsystem.

Two concerns found in the literature were related specifically to the users' need of having more information about the processing of automated HHMT-collected data (Boscart et al., 2008; Ellingson et al., 2011; Tarantini et al., 2019) and the potential use of this data for disciplinary action (Ellingson et al., 2011; Dyson & Madeo 2017; Tarantini et al., 2019). Regarding the first concern, 77.8% of the participants either *"agree"* or *"strongly"* agree that they need more information about the automated HHMT before using it themselves. In addition, 88.9% of the responding participants indicated that it would be either *"very important"* or *"extremely important"* to have information regarding the specific data that the technology would collect, the manner in which this data would be used and the particular roles in the CSH with access to this data. The last type of information (i.e., regarding the roles) seems to have been valued slightly higher than the other two, with 55.6% *"extremely important"* responses for the roles, compared to 44.4% for both the data collected and usage manner. With respect to the second concern, 55.6% of the participants *"strongly agree"* they are worried that sharing individual's HH compliance rates would lead to negative consequences. The rest of the participants either *"neither agree or disagree"* or *"disagree"* with this concern.

While Questions 6 and 7 in the survey were unrelated to the HW-HH-PCs and thus are not discussed here, Questions 8 to 18 referred to the promises (ISO 10001, 6.4.b) of four HW-HH-PCs. These promises included the three identified as feasible by focus group participants (Codes '1', 'A' and 'B' in Table 1). Code '2', which states that the HH compliance rates recorded by the technology would only be shared with the HW, was added to the investigation because it could be significant for HWs, as they have reported concerns about the potential negative consequences of sharing their HH data with managers (Dyson and Madeo, 2017; Tarantini et al., 2019; Blomgren et al., 2021). In addition, this HW-HH-PC could become feasible by adjusting its limitations. For instance, the healthcare organization establishing it could determine that data will only be shared with managers if an individual HH compliance rate below a certain threshold is detected. This would be in line with what the focus group participants reported, since they indicated that in cases of serious non-compliance, the wearable device would be linked to its user anyway.

Questions 8 to 15 were used to assess the importance of the four promises for HWs and whether the HWs would feel more comfortable with the automated HHMT if these promises were to be established. The related results are shown in Table 3.

Table 3. Perceptions of survey participants regarding HW-HH-PC promises

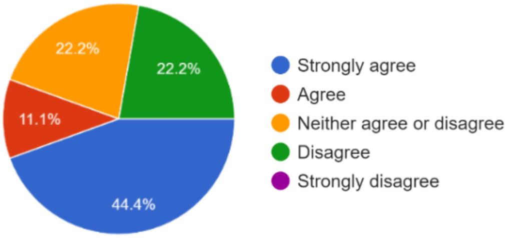
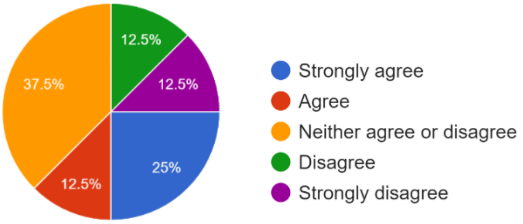
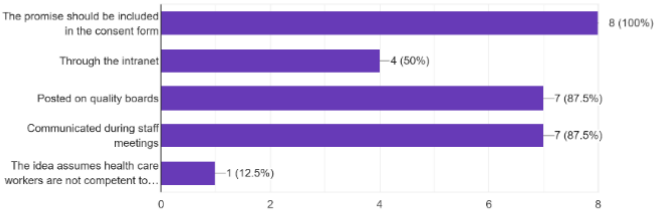
HW-HH-PC Label	**How important would this promise be to you?**	**To what extent do you agree or disagree with: *"I would feel more comfortable with the system if this promise were to be established"***
1		
A		
B		
2		

Code 'A', regarding the roles with access to the collected data, was the most important to the participants. This finding is aligned with the results from the survey question showing that information regarding organizational roles seems to be the most valued by HWs. The second and third most important were Codes '1' and 'B', which concern the purposes for which the collected data would be used and the PII collected by the HHMT, respectively.

The least important code for survey participants was Code '2', which states that a HW's HH compliance rates will only be shared with the HW. It is worth noting that the percentage of participants considering this code as *"extremely important"* coincides with the percentage of participants concerned that sharing an individual's HH compliance rates would lead to negative consequences. The same percentage of respondents (i.e., 55.6%) also *"strongly agreed"* that they would be more comfortable with the HHMT if Code '2' were to be established.

Questions 16 and 17 were used to evaluate other elements of the HW-HH-PCs, namely the hospital's actions if the promise is not fulfilled (ISO 10001, 6.4.e), and the proposed method to provide feedback on the HW-HP-PCs (ISO 10001, 6.4.d). Question 18 was applied to assess potential methods to communicate the HW-HH-PCs to customers (i.e., HWs monitored by the automated HHMT). Table 4 presents the results corresponding to these three questions.

Table 4. Perceptions of survey participants regarding HW-HH-PC elements

Question	Results
Action Box: "The hospital will record information about the incident and initiate a review to determine the measures to be taken." 16) The actions described in the Action Box are adequate.	
"Healthcare workers could provide feedback about these promises and their use by sending an email." 17) The method proposed to provide feedback on promises is adequate.	
18) If the previous promises were to be established, how would you like to be informed about them? (you can select multiple options)	

The results of Questions 16 and 17 presented more dispersion than the answers for questions measuring the importance of the codes. Regarding Question 16 on the hospital's actions if the promises were not fulfilled, 55.5% of the participants either *"agree"* or *"strongly agree"* that these actions would be adequate. Since the survey only included closed-ended questions, it was impossible to know why the participants disagreed with the proposed actions. However, these reasons were explored during the personal interviews with HWs.

With respect to Question 17, which was focused on the method to provide feedback on the HW-HH-PC, only three of the eight respondents *"agree"* or *"strongly agree"* that the email method would be adequate. As in Question 16, the reasons behind these responses were further investigated in the subsequent HWs interviews.

The last survey question (18) was used to verify preferences for informing the HWs regarding the CS codes (ISO 10001, 6.7). All respondents reported that HW-HH-PCs should be included in the consent form, with the majority also indicating preference for communication through boards and meetings. This result validates the consent form as a resource for sharing the codes with the HWs, therefore supporting integration between the ISO 10001 CS system and components of the ISO/IEC 27701 and ISO/IEC 29184 privacy management systems, as proposed in Ortiz and Karapetrovic (2022).

4.3 Interviewing PII principals with respect to the HW-HH-PCs

Personal interviews with two HWs were conducted to verify the importance of five HW-HH-PCs. These five codes included the four HW-HH-PCs evaluated in the electronic survey and the new code proposed in the focus group (Code 'E', please see Table 2). Confirming the importance of the HW-HH-PCs for HWs is critical because effective customer satisfaction guarantees focus on the service aspects that customers value (Hart, 1993; Fabien, 2005; Berman and Mathur, 2014). Since personal interviews included open-ended questions, they allowed investigating the reasons behind specific results obtained in the electronic survey.

As in the survey, the first part of the interview sought to learn whether HWs at the CSH shared the HWs' concerns described in the literature. This part of the interview was essential to validate the existence of the issues that the proposed HW-HH-PCs addressed in the CSH (ISO 10001, 6.2 and 6.3). Verifying that HWs in the CSH had these privacy-related concerns was also important to support the augmentation of the ISO 10001 code system with a privacy subsystem based on ISO/IEC 27701.

Table 5 shows the concerns expressed by the interview participants. Both participants indicated the need to receive information regarding how the hospital would use the collected data to understand the repercussions and risks of using the HHMT. They also mentioned concerns about the punitive use of the collected data, while at the same time pointing out that HWs must be accountable if they do not follow HH guidelines.

Participants One and Two communicated the need to have the information regarding the recipients of the data collected by the HHMT and whether this data would include PII, respectively.

Table 5. Interview participants’ opinions on the automated HHMTs-related concerns

Concern	Participant	Responses
Lack of knowledge regarding the processing of the collected data (Boscart et al., 2008; Ellingson et al., 2011; Tarantini et al., 2019)	One	• Pointed out that they would like to know what the hospital would do with the collected data. • Would want to know what would be the risks associated with using this technology – “*if I do not* [wash my hands], *am I going to lose my job? Or are they going to dock my pay? What is going to happen?”* • Stated that “[they would need information regarding] *who that information goes to”*. “[They would] *not want all* [their] *colleagues to have access to* [the collected data]” and “[would want] *that only people who need to know* [should access it]”.
	Two	• Pointed out that “[they] *would need to* [have information about] *how the* [technology] *works and what the outcome measures are looking to provide information about”*. • “[Would like to know] *why* [the hospital thinks that] *this technology could improve* [patients’ care]”. • Stated that “[they] *would certainly like to know what* [data] *is being collected* [because they would] *like to know if* [their] *name* [was] *associated with it”*. • “[Would like to know] *what repercussions* [would come from implementing the technology, including if there would be] *punitive repercussions*, [for example, whether the collected information would be] *put in* [their] *file* [or would only be used] *to reflect upon and improve quality*”.
Disciplinary use of data (Ellingson et al., 2011; Dyson & Madeo 2017; Tarantini et al., 2019)	One	• Mentioned that “[hospitals need] *to be very careful with* [individual HH compliance rates]”. • Stated that “[this data] *could shame people”* and mentioned that “*people could say*: *X never washes their hands and they will not find a job in another place for that reason*”. • Pointed out that “*at the same time*, [they think that] if [there is someone who is not] *following HH standards, they need to face some consequences”*.
	Two	• Indicated that “[they] *would be concerned if* [the automated HHMT] *was going to be a punitive tool”*. • Pointed out that “[at the same time, they know that highlighting] *specifics* [to an individual] *about their compliance can lead to action*, [and therefore, they] *can see both sides of that”*.

In the second part of the interview, the participants were presented with the five HW-HH-PCs. Both participants were asked about the importance of the related promises and whether the HW-HH-PCs establishment would make them feel more comfortable with the automated HHMT. Participants' answers are shown in Table 6.

As shown in Table 6 and in line with what was expressed by the focus group participants, both interview participants stated that HW-HH-PC-2 should not be established as that would be against the rationale, purpose and effectiveness of the automated HHMT. They considered the other four HW-HH-PCs to be important.

Table 6. Interview participants' opinions regarding the proposed CS codes' importance

HW-HH-PC Label	Important?	Participant	Reasons
1	Yes	One	• Stated that "[this promise would be] *very important* [because HWs] *would know there are specific parameters* [that the hospital] would follow [regarding automated HH monitoring]". • Reported "[they] *would feel much more comfortable* [with the technology if this promise were to be established]".
		Two	• Stated that this promise was important to them. • Pointed out that the hospital must not be distributing the HWs' PII for other reasons that have not been openly communicated to them. According to this participant, HWs need to know what their information is being collected for. • Indicated that "[they] *certainly would be more comfortable if this promise were established"* and stated: *"I do not know about anybody else, but I would be"*.
A	Yes	One	When asked whether this promise was less or more important than the first one, stated: *"both of them are important"*.
		Two	When asked which of the five promises were the most important to them, indicated that *"Code A would probably be the most important because* [HWs would like] *to know who exactly* [would] *identify them"*.
B	Yes	Both	Indicated that promise B is important to them.
2	No	One	• Stated that the technology would only be effective if data is shared with the HW and someone in charge of the HH program or a manager to make the HW accountable for their HH behaviour. • Stated: *"You should get rid of* [this promise]*"*. • Emphasized that *"for the program to work, you have to have accountability built into it"*.
		Two	• Believed that this code should not be established. • Considered that "[this code] *goes against the rationale for having this* [technology] *and defeats* [its] *purpose*". • Pointed out that *"someone* [has to be] *responsible for assessing* [the technology's] *effectiveness*".
E	Yes	One	When asked about the most important promises, stated that promises '1', 'A', 'B' and 'E' were important to them.
		Two	• When presented with code 'E', stated: *"This is even better,* [because it indicates that the hospital] *would only collect the minimum* [relevant] *amount of information"*. • Said*: "This combined with A would be the best code"*.

The interview participants were then asked questions regarding the adequacy and clarity of the remaining four elements of the codes they identified as "important", i.e., for codes '1', 'A', 'B' and 'E'. These elements were the same for all four HW-HH-PCs. Table 7 shows the related responses.

Table 7. Interview participants' opinions regarding the proposed CS codes' elements

HW-HH-PC element	Response	Participant	Reasons
Actions (ISO 10001, 6.4.e)	Adequate?	One	Yes
		Two	- No. - Pointed out that "[the hospital] *could skew* [its internal] *review*". - Considered that "[if the hospital uses a technology that involves] *PII, an external body* [providing] *oversight to be objective* [is needed, since] *the hospital is not going to be a whistleblower on itself".* - Emphasized the need for the hospital to have a notification system to notify this external body and the person affected if they become aware of an incident.
Scope (ISO 10001, 6.4.a)	Clear?	Both	Yes
Terms (ISO 10001, 6.4.c)	Clear?	Both	Yes
Feedback (ISO 10001, 6.4.d)	Adequate?	One	Believed that "*an email* [to the] *HH program coordinator* [was] *good enough* [for providing feedback on the code]".
		Two	- Believed that "*an email could be effective*, [but other methods should also be considered]". - Suggested that an app could be an option depending on the amount of money available for the program. - Pointed out that "*an app* [would be a good option] *because this generation really loves technology".* - Mentioned that there could also be a phone number that HWs could call to speak with a representative of the external body.

As shown in Table 7, Participant Two thinks that the proposed actions for HW-HH-PC-1, -A, -B or -E (ISO 10001, 6.4.e) are inadequate. This participant considered that an external body should be the one conducting the review in cases where the codes are not fulfilled to provide objectivity to the review process. Participant Two also considered that the proposed method for providing feedback on the codes was insufficient. The lack of multiple suggested options may explain why only 37.5% of the survey participants *"strongly agreed"* or *"agreed"* with the method.

The interview participants were also asked how they would like to be informed about these codes, if they were to be established (ISO 10001, clause 6.7). Both participants wanted the HW-HH-PCs to be included in a consent form. Participant One pointed out that this would be a good idea since HWs would then have an opportunity to read these codes and ensure they understand them before signing the form. Participant Two stated that the HW-HH-PCs could be included in the background section of the consent form.

Although Participants One and Two stated that the HW-HH-PCs should be *"definitely"* and *"absolutely"* included in the consent form, respectively, they also pointed out that these codes should be communicated in additional ways. Participant Two mentioned that these codes should be shared using *"multiple approaches"*. Furthermore, both participants cited the inclusion of the HW-HH-PCs in other written documents. Participant One indicated that these codes could be communicated through a flyer or a poster. Both participants also stated that the HW-HH-PCs should be shared during presentations or meetings that provide HWs with opportunities to ask questions. Participant One pointed out that the hospital could prepare a webinar that HWs could access at their convenience to learn about the automated HH monitoring program, including the HW-HH-PCs.

5. Conclusions

Feasibility verification results regarding six privacy-related customer satisfaction codes, as well as an evaluation of their perceived importance were presented in this paper. The codes, named "Healthcare Workers' – Hand Hygiene – Privacy Codes" (HW-HH-PCs), relate to the processing of Personally-Identifiable Information (PII) collected through an automated Health Hygiene Monitoring Technology (HHMT). While the verification was conducted with hospital managers and infection preventionists at a Canadian Case Study Hospital (CSH), the evaluation included HWs at the same hospital.

Four of these codes, namely HW-HH-PC-1, -A, -B and -E, were identified as feasible for establishment and as relevant to HWs. Code 'A' was deemed the most important among the four HW-HH-PCs by HWs participating in an electronic survey and personal interviews. This code concerns the roles with access to the PII collected by the HHMT. HWs also reported that the information about these roles would be the most important information to them. These results are consistent since the code's significance for customers is determined by its focus on the aspects of service appreciated by them (Hart, 1993; Fabien, 2005; Berman and Mathur, 2014).

Using the informed consent form to communicate the HW-HH-PCs to HWs (ISO 10001, 6.7) was deemed feasible by focus group participants. In addition, HWs participating in the online survey and personal interviews wanted the HW-HH-PCs to be communicated through this form. These findings validate the informed consent form as the primary external communication method for the HW-HP-PCs, as proposed in Ortiz & Karapetrovic (2020, 2021 and 2022). In turn, the validation of the informed consent form as a required resource for the codes endorses the augmentation of the ISO 10001 code system with components of the ISO/IEC 27701 and ISO/IEC 29184 privacy subsystems that facilitate the preparation of the consent form, as proposed in Ortiz and Karapetrovic (2022).

Although integrative augmentation of the ISO 10001 customer satisfaction standard with augmentative standards from the ISO information security series in healthcare was analyzed conceptually before (Ortiz and Karapetrovic, 2020, 2021 and 2022), this may be the first article to present empirical data concerning an application of such integrative augmentation. The results demonstrate that components of ISO/IEC 27701 and ISO/IEC 29184 privacy subsystems can support the development of ISO 10001 codes and related resources that are both feasible for the CSH and important for HWs.

The validated HW-HH-PCs presented in this paper may be used by healthcare organizations that are planning to, or have already implemented, an automated HHMT to improve HWs' comfort with this technology and, therefore, increase the likelihood of its successful implementation (Boscart et al., 2008; Meng et al., 2019). Providers of other healthcare-related IoT-based services could slightly adjust these codes and establish them to improve satisfaction as users of various IoT technologies have reported privacy-related concerns in the healthcare context (Birchley et al., 2017; Lowens et al., 2017; Boonstra et al., 2018; Pal et al., 2018; Grant et al., 2019; Auepanwirikayul, 2020).

Regarding the limitations of this research, the electronic survey and online interviews included a small number of HWs. These small samples might not have captured the existing diversity of opinions among the CSH's HWs regarding the proposed codes and the related resources (Malterud et al., 2016). Another limitation was that the CSH had only implemented the HHMT as a pilot project.

In future research, the proposed codes should be validated with a larger sample of HWs, which would allow confirming, for example, the need to have an external body in charge of the review process in cases when the codes are not met as pointed out by an interview participant. Implementing these codes at various hospitals should be interesting in order to compare their impact on organizations with different characteristics, such as organizational cultures (Chang et al., 2015; Iwaya et al., 2022). Furthermore, adjustment of the proposed codes for different IoT-based technologies implemented in healthcare, such as fall detection systems (Li et al., 2014; De Quadros et al., 2018) and health monitoring systems (Pardeshi et al., 2017; Swaroop et al., 2019), and for IoT applications in other contexts, such as home automation (Jabbar et al., 2019; Stolojescu-Crisan et al., 2021), shopping (Li et al., 2017; Hussien et al., 2020), and education (Zhuang et al., 2021; Gao, 2022), can be investigated. Finally, integrative augmentation between the ISO 10001 CS management system and the ISO/IEC 27701 and ISO/IEC 29184 privacy subsystems could be further expanded by adding other relevant standards, such as the newly published ISO/IEC 27400:2022, which provides guidelines related to information security and privacy in the IoT context.

Acknowledgment:
The authors recognize Alberta Health Services; the National Fund for Scientific, Technological Development and Technological Innovation (FONDECYT), the funding branch of the National Council for Science, Technology and Technological Innovation (CONCYTEC) Peru; and Natural Sciences and Engineering Research Council (NSERC) of Canada.

References:

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception. *IEEE Access*, *7*, 111341-111354. http://dx.doi.org/10.1109/ACCESS.2019.2904006

Auepanwiriyakul, C., Waibel, S., Songa, J., Bentley, P., & Faisal, A. A. (2020). Accuracy and acceptability of wearable motion tracking for inpatient monitoring using smartwatches. *Sensors*, *20*(24), 7313. http://dx.doi.org/10.3390/s20247313

Bellou, V. (2010). The role of learning and customer orientation for delivering service quality to patients. *Journal of Health Organization and Management*, *24*(4), 383-395, http://dx.doi.org/10.1108/14777261011064995

Benudis, A., Stone, S., Sait, A. S., Mahoney, I., Price, L. L., Moreno-Koehler, A., Anketell, E., & Doron, S. (2019). Pitfalls and unexpected benefits of an electronic hand hygiene monitoring system. *American Journal of Infection Control*, *47*(9), 1102-1106. http://dx.doi.org/10.1016/j.ajic.2019.03.011

Berman, B., & Mathur, A. (2014). Planning and implementing effective service guarantee programs. *Business Horizons*, *57*(1), 107-116. http://dx.doi.org//10.1016/j.bushor.2013.10.005

Berry, L. L. (2019). Service guarantees have a place in health care. *Annals of Internal Medicine*, *170*(2), 116-117. http://dx.doi.org/10.7326/M18-2412

Birchley, G., Huxtable, R., Murtagh, M., Ter Meulen, R., Flach, P., & Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC Medical Ethics*, *18*(1), 1-13. https://dx.doi.org/10.1186/s12910-017-0183-z

Blomgren, P.-O., Lytsy, B., Hjelm, K., & Swenne, C.L. (2021). Healthcare workers' perceptions and acceptance of an electronic reminder system for hand hygiene. *Journal of Hospital Infection*, *108*, 197-204. http://dx.doi.org/10.1016/j.jhin.2020.12.005

Boonstra, T. W., Nicholas, J., Wong, Q. J., Shaw, F., Townsend, S., & Christensen, H. (2018). Using mobile phone sensor technology for mental health research: Integrated analysis to identify hidden challenges and potential solutions. *Journal of Medical Internet Research*, *20*(7), e10131. http://dx.doi.org/10.2196/10131

Boscart, V. M., McGilton, K. S., Levchenko, A., Hufton, G., Holliday, P., & Fernie, G. R. (2008). Acceptability of a wearable hand hygiene device with monitoring capabilities. *Journal of Hospital Infection*, *70*(3), 216-222. http://dx.doi.org/10.1016/j.jhin.2008.07.008

Boshoff, C. (2002). Service advertising: an exploratory study of risk perceptions. *Journal of Service Research*, *4*(4), 290-298.

Boyce, J. M. (2008). Hand hygiene compliance monitoring: current perspectives from the USA. *Journal of Hospital Infection*, *70,* 2-7. http://dx.doi.org/10.1016/S0195-6701(08)60003-1

Boyce, J. M., Cooper, T., Yin, J., Li, F. Y., & Arbogast, J. W. (2019). Challenges encountered and lessons learned during a trial of an electronic hand hygiene monitoring system. *American Journal of Infection Control*, *47*(12), 1443-1448. http://dx.doi.org/10.1016/j.ajic.2019.05.019

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems, 115*(1), 88-106. http://dx.doi.org/10.1108/IMDS-07-2014-0197

Conway, L. J. (2016). Challenges in implementing electronic hand hygiene monitoring systems. *American Journal of Infection Control*, *44*(5), e7-e12. http://dx.doi.org/10.1016/j.ajic.2015.11.031

Cook, S. (2020). How to hold adequate data. *BDJ In Practice*, *33*(6), 33. http://dx.doi.org/10.1038/s41404-020-0419-3

Courneya, P. T., Palattao, K. J., & Gallagher, J. M. (2013). HealthPartners' online clinic for simple conditions delivers savings of $88 per episode and high patient approval. *Health Affairs*, *32*(2), 385-392. http://dx.doi.org/10.1377/hlthaff.2012.1157

De Quadros, T., Lazzaretti, A. E., & Schneider, F. K. (2018). A movement decomposition and machine learning-based fall detection system using wrist wearable device. *IEEE Sensors Journal, 18*(12), 5082-5089. http://dx.doi.org/10.1109/JSEN.2018.2829815

Dyson, J., & Madeo, M. (2017). Investigating the use of an electronic hand hygiene monitoring and prompt device: influence and acceptability. *Journal of Infection Prevention*, *18*(6), 278-287, http://dx.doi.org/10.1177/1757177417714045

Ellingson, K., Polgreen, P. M., Schneider, A., Shinkunas, L., Kaldjian, L. C., Wright, D., ... & Sinkowitz-Cochran, R. (2011). Healthcare personnel perceptions of hand hygiene monitoring technology. *Infection Control & Hospital Epidemiology*, *32*(11), 1091-1096. http://dx.doi.org/10.1086/662179

Fabien, L. (2005). Design and implementation of a service guarantee. *Journal of Services Marketing*, *19*(1), 33-38. https://dx.doi.org/10.1108/08876040510579370

Franklin, M. A. (2018). Healthcare's future: strategic investment in technology. *Frontiers of Health Services Management*, *34*(3), 16-28, http://dx.doi.org/10.1097/HAP.0000000000000025

Gao, W. (2022). Designing an interactive teaching model of English language using Internet of Things. *Soft Computing*, 1-11. http://dx.doi.org/10.1007/s00500-022-07156-y

Grant, S., Blom, A. W., Craddock, I., Whitehouse, M., & Gooberman-Hill, R. (2019). Home health monitoring around the time of surgery: qualitative study of patients' experiences before and after joint replacement. *BMJ Open*, *9*(12), e032205. http://dx.doi.org/10.1136/bmjopen-2019-032205

Guo, M., Wagner, M., & West, C. (2004). Outpatient clinic scheduling: a simulation approach. *Proceedings of the 2004 Winter Simulation Conference, 2*, 1981-1987. https://doi.org/10.1109/WSC.2004.1371559

Hart, C. W., Schlesinger, L. A., & Maher, D. (1992). Guarantees come to professional service firms. *MIT Sloan Management Review*, *33*(3), 19-29.

Hart, C.W.L. (1993). Satisfaction guaranteed. *Small Business Reports*, *18*(11), 19-23.

Hogreve, J., & Gremler, D.D. (2009). Twenty years of service guarantee research: a synthesis. *Journal of Service Research*, *11*(4), 322-343. https://dx.doi.org/10.1177/1094670508329225

Hussien, N., Ajlan, I., Firdhous, M. M., & Alrikabi, H. (2020). Smart shopping system with RFID technology based on internet of things. *International Journal of Interactive Mobile Technologies, 14*(4), 17-29. https://dx.doi.org/10.3991/ijim.v14i04.13511

Information Commissioner's Office. (2021, January 1). *Guide to the general data protection regulation (GDPR)*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

International Organization for Standardization. (2011*). Information technology - security techniques - privacy framework* (ISO/IEC Standard No. 29100:2011). https://www.iso.org/standard/45123.html

International Organization for Standardization. (2013*). Information technology - security techniques – information security management systems – requirements* (ISO/IEC Standard No. 27001:2013). https://www.iso.org/standard/54534.html

International Organization for Standardization. (2018a). *Information technology — service management — part 1: service management system requirements* (ISO Standard No. 20000-1:2018). https://www.iso.org/standard/70636.html

International Organization for Standardization. (2018b). *Quality management — customer satisfaction — guidelines for codes of conduct for organizations* (ISO Standard No. 10001:2018). https://www.iso.org/standard/71579.html

International Organization for Standardization. (2019*). Security techniques – extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines* (ISO/IEC Standard No. 27701:2019). https://www.iso.org/standard/71670.html

International Organization for Standardization. (2020*). Information technology – online privacy notices and consent* (ISO/IEC Standard No. 29184:2020). https://www.iso.org/standard/70331.html

Iversen, A. M., Kavalaris, C. P., Hansen, R., Hansen, M. B., Alexander, R., Kostadinov, K., ... & Ellermann-Eriksen, S. (2020). Clinical experiences with a new system for automated hand hygiene monitoring: a prospective observational study. *American Journal of Infection Control*, *48*(5), 527-533. http://dx.doi.org/10.1016/j.ajic.2019.09.003

Iwaya, L. H., Iwaya, G. H., Fischer-Hübner, S., & Steil, A. V. (2022). Organisational privacy culture and climate: a scoping review. *IEEE Access*, *10*, 73907-73930. http://dx.doi.org/10.1109/ACCESS.2022.3190373

Jabbar, W.A., Kian, T. K., Ramli, R. M., Zubir, S. N., Zamrizaman, N. S., Balfaqih, M., Shepelev, V., & Alharbi, S. (2019). Design and fabrication of smart home with Internet of Things enabled automation system. *IEEE Access, 7*, 144059-144074. http://dx.doi.org/10.1109/ACCESS.2019.2942846

Karapetrovic, S. (2005). IMS in the M(E)SS with CSCS. *Total Quality Management and Excellence*, *33*(3), 19-25.

Kashyap, R. (2001). The effects of service guarantees on external and internal markets. *Academy of Marketing Science Review*, *10*(1), 1-19.

Khan, M.A.R. (2016). *An ISO 10000-based Patient Satisfaction Framework*. [Doctoral dissertation, University of Alberta]. ERA: Education and Research Archive. https://doi.org/10.7939/R3KD1QW8V

Khan, M. A. R., & Karapetrovic, S. (2013). Implementing an ISO 10001-based promise in inpatients care. *International Journal for Quality Research*, *7*(3), 335-346.

Khan, M. A. R., & Karapetrovic, S. (2015). Establishing an ISO 10001-based promise in inpatients care. *International Journal of Health Care Quality Assurance*, *28*(2), 100-114. http://dx.doi.org/10.1108/IJHCQA-05-2013-0050

Kumar, P., Kalwani, M. U., & Dada, M. (1997). The impact of waiting time guarantees on customers' waiting experiences. *Marketing Science*, *16*(4), 295-314.

Lee, K. & Khan, M. A. (2012). Exploring the impacts of service guarantee strategy. *Journal of Travel & Tourism Marketing*, *29*(2), 133-146. http://dx.doi.org/10.1080/10548408.2012.648530

Levchenko, A. I., Boscart, V. M., & Fernie, G. R. (2014). Automated monitoring: a potential solution for achieving sustainable improvement in hand hygiene practices. *CIN: Computers, Informatics, Nursing, 32*(8), 397-403. https://doi.org/10.1097/CIN.0000000000000067

Li, Z., Huang, A., Xu, W., Hu, W., & Xie, L. (2014). Fall perception for elderly care: a fall detection algorithm in smart wristlet mhealth system. *2014 IEEE International Conference on Communications (ICC)* (pp. 4270-4274). IEEE.

Li, R., Song, T., Capurso, N., Yu, J., Couture, J., & Cheng, X. (2017). IoT applications on secure smart shopping system. *IEEE Internet of Things Journal*, *4*(6), 1945-1954. http://dx.doi.org/10.1109/JIOT.2017.2706698

Lowens, B., Motti, V. G., & Caine, K. (2017). Wearable privacy: skeletons in the data closet. *2017 IEEE International Conference on Healthcare Informatics (ICHI)*, 295-304. https://doi.org/10.1109/ICHI.2017.29

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: guided by information power. *Qualitative Health Research*, *26*(13), 1753-1760. https://doi.org/10.1177/1049732315617444

Manolitzas, P., Fortsas, V., Grigoroudis, E., & Matsatsinis, N. (2014). Internal customer satisfaction in healthcare organizations: a multicriteria analysis approach. *International Journal of Public Administration*, *37* (10), 646-654. https://doi.org/10.1080/01900692.2014.903267

McGuckin, M., & Govednik, J. (2015). A review of electronic hand hygiene monitoring: considerations for hospital management in data collection, healthcare worker supervision, and patient perception. *Journal of Healthcare Management*, *60*(5), 348-361. http://dx.doi.org/10.1097/00115514-201509000-00009

Meng, M., Sorber, M., Herzog, A., Igel, C., & Kugler, C. (2019). Technological innovations in infection control: a rapid review of the acceptance of behavior monitoring systems and their contribution to the improvement of hand hygiene. *American Journal of Infection Control*, *47*(4), 439-447. http://dx.doi.org/10.1016/j.ajic.2018.10.012

Ortiz, M. B., & Karapetrovic, S. (2020). Preliminary Model for IoT-Related ISO 10000 Integrative Augmentation. In P. Sampaio, P. Domingues, C. Cubo, M. Cabecinhas, M. Casadesús, F. Marimon, A.R. Pires, & P. Saraiva (Eds.), *Proceedings Book of the 4th International Conference on Quality Engineering and Management, 2020* (pp.715-730). International Conference on Quality Engineering and Management.

Ortiz, M. B., & Karapetrovic, S. (2021). Two examples of IoT-related healthcare worker's hand hygiene privacy codes. *24th Excellence in Services International Conference (EISIC).* https://sites.les.univr.it/eisic/wp-content/uploads/2021/10/3-Belen-Ortiz-Karapetrovic.pdf

Ortiz, M. B., & Karapetrovic, S. (2022). Developing Internet of Things-related ISO 10001 Hand Hygiene Privacy Codes in Healthcare. *The TQM Journal*, ahead-of-print (ahead-of-print). https://doi.org/10.1108/TQM-03-2022-0081

Pal, D., Funilkul, S., Charoenkitkarn, N., & Kanthamanon, P. (2018). Internet-of-things and smart homes for elderly healthcare: an end user perspective. *IEEE Access, 6*, 10483-10496. http://dx.doi.org/10.1109/ACCESS.2018.2808472

Pardeshi, V., Sagar, S., Murmurwar, S., & Hage, P. (2017). Health monitoring systems using IoT and Raspberry Pi - a review. *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp.134-137). http://dx.doi.org/10.1109/ICIMIA.2017.7975587

Pong, S., Holliday, P., & Fernie, G. (2018). Effect of electronic real-time prompting on hand hygiene behaviors in health care workers. *American Journal of Infection Control*, *46*(7), 768-774. http://dx.doi.org/10.1016/j.ajic.2017.12.018

Raffio, T. (1992). Quality and delta dental plan of Massachusetts. *MIT Sloan Management Review*, *34* (1), 101-110.

Sax, H., Allegranzi, B., Chraïti, M. N., Boyce, J., Larson, E., & Pittet, D. (2009). The World Health Organization hand hygiene observation method. *American Journal of Infection Control*, *37*(10), 827-834. http://dx.doi.org/10.1016/j.ajic.2009.07.003

Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784. http://dx.doi.org/10.3390/s21113784

Swaroop, K. N., Chandu, K., Gorrepotu, R., & Deb, S. (2019). A health monitoring system for vital signs using IoT. *Internet of Things, 5,* 116-129. http://dx.doi.org/10.1016/j.iot.2019.01.004

Tarantini, C., Brouqui, P., Wilson, R., Griffiths, K., Patouraux, P., & Peretti-Watel, P. (2019). Healthcare workers' attitudes towards hand-hygiene monitoring technology. *Journal of Hospital Infection, 102*(4), 413-418. http://dx.doi.org/10.1016/j.jhin.2019.02.017

Thomassen, J. P., Ahaus, K., & Van de Walle, S. (2014). Developing and implementing a service charter for an integrated regional stroke service: an exploratory case study. *BMC Health Services Research*, *14*, 1-11. http://dx.doi.org/10.1186/1472-6963-14-141

Virtuwell (2022a). *How it works*. https://www.virtuwell.com/how-it-works (accessed by 10 August 2022)

Virtuwell (2022b). *Your favorite online clinic*. https://www.virtuwell.com/ (accessed by 10 August 2022)

Wirtz, J., Kum, D., & Lee, K. S. (2000). Should a firm with a reputation for outstanding service quality offer a service guarantee?. *Journal of Services Marketing*, *14*(6), 502-512. http://dx.doi.org/10.1108/08876040010347615

World Health Organization. (2009, January 15). *WHO guidelines on hand hygiene in health care*. https://www.who.int/publications/i/item/9789241597906

Zhuang, L., Hsu, C. H., & Kumar, P. M. (2021). IoT based multimodal social interaction activity framework for the physical education system. *Wireless Personal Communications*, 1-17. http://dx.doi.org/10.1007/s11277-021-09014-w

María Belén Ortiz
Universidad de Ingeniería y Tecnología - UTEC
Lima, Lima
Peru
mortizg@utec.edu.pe
ORCID 0000-0002-9785-0022

Stanislav Karapetrovic
University of Alberta,
Edmonton, Alberta
Canada
stanislav@ualberta.ca
ORCID 0000-0001-8162-9705