

Recording of Personal Health Information in the Age of Smartphones

Raghav V. Sampangi, *Dalhousie University* Carla Ann Heggie, *Dalhousie University*
Simeon Kanev, *Alliance for Healthier Communities*

Abstract

The ubiquity of smartphones and other mobile devices offers a range of conveniences, including giving patients the ability to record discussions during healthcare appointments that may contain medical advice and opinion, which constitute personal health information (PHI). We explore the dimensions of recording PHI, with a focus on privacy, ethics, and security aspects of these types of recordings in the Canadian context. We note that there does not appear to be much guidance in healthcare policy which dictates the boundaries of the relationship between the patient and healthcare professional. In Canadian law, the concept of one party consent allows patients to record interactions with healthcare professionals without the need for their consent. While not illegal, this could result in issues such as erosion of trust, changed power dynamics, accountability, etc. In this paper, we recommend guidelines, founded in Privacy by Design fundamental principles, for application developers to inform patients or caregivers about the potential risks of recording their interactions with healthcare professionals. Our next steps are to evaluate the guidelines we recommend, to continue exploring the various dimensions around recording and PHI, and to develop and evaluate technological solutions for the same.

1. Overview

“*Privacy is the right to be let alone*” - Warren and Brandeis [1] included a definition of privacy by Judge Cooley as such in their 1890 Harvard Law Review article. This definition has stood the test of time even though the concept of privacy (and ethics and security in relation to privacy), the needs of individuals and their perceptions, and privacy law have evolved. Individuals now have the luxury of taking several aspects of convenience for granted, such as carrying a mobile device with them in their daily activities. We use the generic term, mobile device, because it encompasses the many devices people can carry on their person, e.g., phones, wearable devices,

recording devices, etc. and slightly larger mobile devices such as tablets and laptops. This convenience allows us access to, and the ability to control, our personal information at our fingertips. And this also provides the mechanism to create new information in different contexts, which brings us to the focus in our work.

Our work explores the privacy, ethical, and security aspects of digital information recording by patients and their caregivers, using mobile devices, during appointments with healthcare professionals. We explore the impact of this on the management of *personal health information* (PHI) by both the patient and the healthcare professional. Such recordings are further impacted by various privacy laws and technological aspects, such as data storage and management. Privacy legislation speaks to the collection, use, and disclosure of personal information. Specifically in the healthcare sector, PHI protection is mandated within the circle of care.

We also focus on the legislative and ethical accountability for upholding the privacy rights of patients and the transparency of healthcare professionals. Of particular interest to us is the impact of patients and caregivers recording PHI on their personal devices, which may not be secure, or use cloud-based storage that may be governed by laws of another jurisdiction. Indeed, the patient may unknowingly breach their own privacy.

Considering a comprehensive perspective of the interaction between patients, caregivers, and their healthcare providers, we explore opportunities to improve the trust and communication in this relationship. With this perspective and based on lessons learned, we also present guidelines for app developers which (a) aim to help keep the user (patient or healthcare professional) informed about privacy implications when they initiate a recording, and (b) satisfy the Privacy by Design [2] guidelines.

In the remainder of this paper, we discuss the background of this topic (Section 2), discuss Privacy by Design in this context (Section 3), and elaborate on the risks, presenting risk mitigation guidelines for app developers (Section 4).

2. Background

Given the growth of mobile devices, the ability of individuals to record any manner of interactions has increased exponentially. In the area of healthcare, these devices provide an opportunity for patients and their caregivers to record interactions with their healthcare providers.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 08 -- 10, 2021, Santa Clara, CA, USA.

Individuals may record medical appointments for various reasons, including convenience, accuracy, clarification, memorability (record keeping), accountability and communication. These reasons may be different depending upon the role of the person recording. For example, patients may wish to self-document or record the advice for future reference. Both clinicians and patients may require the recordings for their records. Recordings may also be used by clinicians for teaching or research purposes, with appropriate consent. Ultimately, recording of PHI of any kind speaks to accountability of all parties.

From an ethical standpoint, we need to explore the concept of whether such recordings result in the overall improvement or enhancement of patient care. There is a perception that some healthcare providers may negatively view patients recording an appointment [3].

2.1. Issues with Recording PHI

Issues or concerns around recording PHI may depend upon the approach taken by the person recording. If the recording is done with the knowledge of the other entity, there should not be any issues.

The relationship between a patient and their healthcare provider is, and should be, one of trust. Should one of the entities records while the other is uncomfortable, such trust may be broken. For example, interactions with healthcare providers may also feature power dynamics, in which the power is perceived to reside with the healthcare provider. The healthcare provider may not be comfortable with their advice being recorded, either due to the power dynamics or with them feeling threatened by possible legal action. This may lead the patient or their caregiver to attempt to record without their knowledge (i.e., covertly), leading to a breach of trust. Alternatively, if they are aware that the other party is recording, either party may tailor their behaviours and/or responses due to the *panopticon effect* [4]. As such, clinicians tend to be very cautious about being recorded as they most often associate a recording with potential malpractice investigations, legal action and scrutinization of their work.

This leads us to the ethical discussion as to whether this is a legislative or moral argument. Under privacy legislation [5][6][7][8][9][10][11], the opinion of the clinician about an individual's health condition is the personal information of the patient. Therefore, a patient is recording their own personal health information, which is not a privacy issue.

However, there is a moral aspect to consider here as well. In Canada, it is not illegal to record a conversation with other parties as long as one of the parties in the conversation consents to the recording (Section 183.1 Criminal Code of Canada [12]), a stance that has been upheld by Canadian courts [3]. So, effectively, if the patient chooses to covertly record the interaction, they are performing an action that is not

illegal, but which could lead to possible breach of trust. Healthcare professionals, on the other hand, are governed by strict professional codes of conduct, which prevent them from covertly recording interactions with patients [13].

2.2. Literature Review

Our intent is to limit this work to healthcare in the Canadian context, as legal implications, both for healthcare and privacy, differ in different countries. However, we explore some research and application development done globally through a quick scan of the literature to understand different perspectives that have been addressed in this domain. This snapshot, if you will, of the literature presents a summary of work done on specific parts of this larger problem domain. This has led us to believe that a comprehensive perspective on privacy in recording of PHI is worthy of further investigation.

To the best of our knowledge, studies in the Canadian context in this domain consider specific aspects, such as the work by Oyedokun et al. [14], but in our opinion, a broader exploration is necessary to scope out the issue and develop user-centric solutions.

One of the studies that has considered one aspect of patients or their caregivers recording their healthcare experiences in the emergency department was conducted by Oyedokun et al. [14]. Specifically, they looked into patients recording minor procedures performed in the emergency (e.g., suturing) with an intention of sharing.

Globally, people have explored the aspect of privacy and PHI from different perspectives, including the work by Henken et al. [15] in the Netherlands, who studied the implications of the law on video recordings from a clinician's perspective. They specifically studied endoscopic recordings and their use in patient healthcare, but also identify other purposes for recording in a clinical setting such as surveillance, research, education, etc. Their study acknowledges that the reasons for recordings may differ given different contexts and modes of recording. For example, endoscopic recordings may be part of the patient's diagnosis and treatment.

Tsulukidze et al. have explored recordings of PHI from two perspectives: as an underutilized asset in medical intervention [16] and about the reasons why patients record clinical encounters covertly [17]. Through their scoping review [16], they identified the value in sharing the recordings of clinical consultations with patients. Patients were found to use the recordings for sharing them with their doctors, friends and family as well as for reviewing them as part of ongoing healthcare. Their study acknowledged that patients benefit from receiving such recordings as they are able to recall and understand more information. The recordings were also found to alleviate psychological impact in some patients.

In their work on why patients record their clinical interactions covertly [17], they analyzed content on the Web (e.g., through blogs) shared by patients and clinicians about their perspectives on recording conversations. Their analysis found that both patients and clinicians had conflicting reactions to the concept of recording. While some of them looked at it from a negative perspective, considering the possible erosion of trust due to covert recording, many others provided positive opinions, considering the feeling of empowerment experienced by patients in managing their healthcare. This aspect of empowerment was also found in a survey study conducted by Elwyn et al. [18].

With a focus on patient-centered care and in response to patients choosing to record their clinical appointments, the work by Lipson-Smith et al. [19] developed an app (SecondEars) to facilitate such recordings. This app was developed through co-design activities with patients in Australia. Their app allowed oncology patients to audio record interactions with different specialists and store these recordings in one central location.

While the reasons used by patients and clinicians for recordings may differ, it is clear that there is a growing need to support such recordings in ongoing patient care as well as for record keeping and education. Ultimately, there has to be a balance between the need of the patients to record their PHI and the clinicians need to trust that the recording is being done in a legal and ethical manner.

2.3. How do people record?

In this section, we consider two technology options that could be used by patients and caregivers to record conversations: (a) smartphones, and (b) portable recording devices.

We limit our focus to recording mechanisms used by patients and their caregivers because official recordings by healthcare professionals are expected to follow the privacy and healthcare regulations in their countries for collection, use, and disclosure of PHI while there are currently no such known legislations for patients, which lead to increased risks.

(a) Smartphones: Being one of the most ubiquitous categories of personal devices in 2021, smartphones are likely the easiest devices to use for recording conversations. The majority of the global population use these devices [20] and this combined with prevalence of apps to record phone conversations [21] and other voice-based conversations [22], they become a convenient device on which to record interactions.

A typical recording app [23][24] records the conversation and stores it on the physical device, using the on-device memory. However, with a focus on ease of use (both of the app and the phone) and easy access to a user's creations, these recordings may be backed-up by the user in either a local storage device or in a remote server (a.k.a. cloud storage). Depending on the

mobile device being used, the user may be able to use shortcuts available (e.g., iOS shortcuts) in the operating system to initiate recording or they may have to start recording using a recording app (e.g., VoiceRecorder on Android, Voice Memos on iOS).

When the user is recording an interaction, the use of a smartphone for recording can either go unnoticed or be obvious (e.g., if the phone is in the user's chest pocket with the camera facing the other person in the conversation, etc.).

(b) Portable recording devices: These are small recording devices that may sometimes look like everyday gadgets (e.g., a pen). These devices could have video and/or audio recording capabilities [25]. While these devices are less ubiquitous as compared to smartphones, the devices that look like every day gadgets are less obvious and can easily go unnoticed during a conversation (e.g., a pen may seem to be more 'natural' as an accessory that goes in the chest pocket and can therefore go unnoticed during covert recordings).

A typical recording device has the following components:

- Recording sensor (microphone for voice, optionally camera for video)
- On-device storage (with some devices offering options to extend storage through SD cards)
- Computer interface (to connect with a laptop/desktop computer to transfer recording)
- Functionality for the device in case of covert recordings (e.g., ink and the mechanism to write for a recording device that looks like a pen, etc.)

The recording can be initiated differently in different devices. For example, buttons available on pens or other devices to turn on the recording.

This review of recording devices is based on the currently available technologies. We acknowledge that such devices are increasingly more sophisticated, making it easier for users to record, store, and share interactions.

2.4. The Players

In this section, we identify the entities who may be impacted by recording PHI.

(a) Patients and caregivers. The main reason patients may choose to record their healthcare interactions is recollection of what has been discussed [26][14], in addition to other reasons (e.g., sharing with others) that we have identified earlier in this paper. The amount of information remembered could also be dependent on the severity/negativity of the information provided by the clinician. In some circumstances, caregivers may record interactions on behalf of the patient.

(b) Healthcare professionals: Among some healthcare professionals, there is a negative perception that recordings could be used for litigation [27], while some believe that recordings increase accountability and support for patients.

(c) Privacy professionals: For privacy professionals, recordings of PHI are yet again another venue for the collection, use or disclosure of personal information. A privacy professional would be mindful of the potential for a privacy breach (e.g., in the event of an emergency procedure being recorded that could inadvertently record the diagnosis and/or other information of a neighbouring patient).

3. Risks and Mitigation

In this section, we identify risks from the perspectives of both the healthcare professional and the patient and identify techniques to mitigate such risks. As identified in the overview of Section 2.3, we limit our focus of risks in the event patients and caregivers record their interactions with the healthcare professional. Learning from our literature review, the risks and with a focus on keeping the patient informed about privacy risks, we also present guidelines for developers of recording apps.

3.1. Risks

Risk #1: Perception of knowledge. The recording of an interaction may lead to patients or caregivers believing that they have all the information they need, and there is a risk that the information may be taken out of context.

Risk #2: Possible litigation. Patients or caregivers may use the recordings, in part or full, to pursue legal action against the healthcare professional.

Risk #3: Breach of trust and confidentiality. The healthcare provider may perceive the recording as questioning their professionalism. The patients may be recording because they do not trust the professional.

Risk #4: Power dynamics. Historically, doctors and specialists are perceived to hold a position of power. By recording, patients may feel that they are taking on some control of their own healthcare, which could be perceived as shifting the power dynamic in their favour. With one-party consent to initiate recordings being not illegal in Canada, this may mean that healthcare professionals may be legally recorded without their knowledge or consent [3].

Risk #5: Stress. Being recorded subjects the healthcare professional to increased stress, as they may feel that their work is being scrutinized, leading them to be cautious with their words and advice.

Risk #6: Lack of accountability. Healthcare professionals are accountable under law to ensure the privacy of their patients. Patients, on the other hand, are not accountable under privacy legislation. There is no guarantee or guidelines for patients to

follow regarding the use, storage, and disclosure of the recordings.

Risk #7: Refusal to treat. The healthcare professional may feel threatened and may refuse treatment to the patient if they become aware of the patient recording their interactions.

Risk #8: Storage of PHI. The patient may be unaware of the necessity to store their information in a secure manner and may result to using often free cloud services for storage. This leads to a lack of accountability and possible privacy breach.

Risk #9: Accidental loss of PHI. There is a risk of loss of PHI and potential privacy breach in the event of the theft of the patient's or caregiver's phones/recording devices, illegitimate access (a.k.a. hacking) of information on personal devices or cloud servers, or erroneous deletion.

3.2. Risk Mitigation through Communication

Open and clear communication by the recording party with the other is essential to ensure the trust in the relationship. If the recording party is the healthcare professional, they are required to get the consent of the patient and their caregivers before a recording can begin. Since no such requirement exists for patients and their caregivers, it might benefit them to explain the reasoning to the healthcare professional and seek their permission before recording the interaction. This would minimize the risk to the healthcare professional as they would be aware of the recording taking place and will further strengthen the relation of trust with the patient.

Clear policies implemented at the institutional level and communicated clearly would further help setting expectations for both healthcare professionals and patients/caregivers. If healthcare professionals refuse a recording request, they should accommodate this in an alternative way such as providing a clear written clinical summary of the information discussed/guidance provided, as identified by Nolan et al. [3].

As we see in this section, several risks can be mitigated through effective communication. However, if the communication is either one-time or in locations that may not be available/accessible just-in-time when patients attempt a recording, considering technology-based solutions may need to be considered. With this in mind and considering the Privacy by Design (PbD) fundamental principles for IT system design [2], we recommend guidelines in the next section that developers could use when developing or updating apps that support recording.

3.3. Risk Mitigation through Recording App Features: Guidelines for Developers

We develop these guidelines with the perspective that a recording app should inform the patient or caregiver about potential risks of proceeding with the recording, especially in the context of PHI. Figure 1 illustrates the approach we recommend for developers to consider when developing or

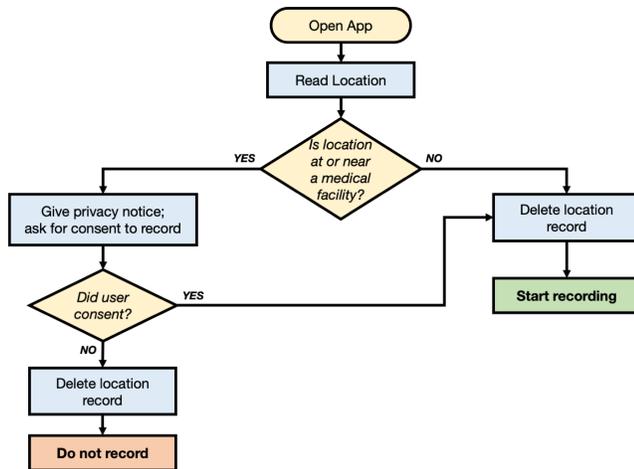


Figure 1. Flowchart illustrating our recommendation to present context-specific information to the user to seek their consent before recording.

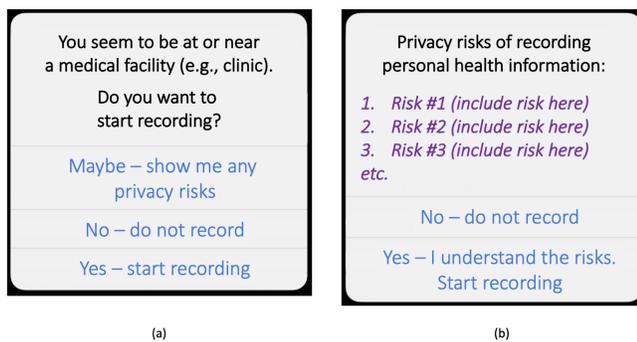


Figure 2. Sample illustrations of privacy notice and information dialog. (a) illustrates a sample privacy notice giving the user the choice to seek additional information about risks, to record, or not to record. (b) illustrates a sample information dialog that can be displayed if the user chooses the first option in (a), i.e., Maybe – show me any privacy risks.

updating apps that support recordings. The guidelines are as follows:

(a) Identify whether the user is at or near a medical facility. This is essential to verify if they are recording something at a healthcare facility or elsewhere. This is essential for the rest of the guidelines, which also becomes a foundation to meet the PbD principles through such an app or feature.

(b) Give privacy notice and seek explicit consent for recording. If the user is at or near a healthcare facility, as inferred from the location, give the user a privacy notice. Sample privacy notices are illustrated in Figures 2 and 3. It is important to seek explicit consent from the user to record in such a scenario because they need to be aware of the risks before initiating the recording. Note that this guideline considers that

a privacy notice may not necessary elsewhere, when the user may be recording for personal reasons, but assumes that recordings at or near healthcare facilities may involve PHI. This guideline is founded on PbD principles #1 (proactive not reactive; preventative not remedial), #2 (privacy as the default setting) and #3 (privacy embedded into design).

(c) If the user consents, delete location record and begin recording. The location record is not needed after their location is inferred and a decision has been made. Therefore, delete the location record before beginning the recording. This guideline is founded on PbD principles #4 (full functionality – positive-sum, not zero-sum) and #7 (respect for user privacy – keep it user-centric).

(d) If the user does not consent, delete location record and take them to the app main screen. As with (c) the location record is not needed after their location is inferred and a decision has been made. If the user chooses to not go ahead with the recording, delete the location record and take the back to the app’s main screen (or alternatively the phone’s home screen) as they do not need to record. This guideline is founded on PbD principles #4 (full functionality – positive-sum, not zero-sum) and #7 (respect for user privacy – keep it user-centric).

(e) Present the risks in simple language. This is a critical aspect to consider as risk information presented in legal jargon may themselves pose the risk of being ignored by the user, as is observed with user behaviour around EULAs (End User License Agreements). This guideline is founded on PbD principles #6 (visibility and transparency – keep it open) and #7 (respect for user privacy – keep it user-centric).

All these guidelines are developed with a focus on PbD principles #6 (visibility and transparency – keep it open) and #7 (respect for user privacy – keep it user-centric). We have not explicitly considered PbD principle #5 (end-to-end security – full lifecycle protection) in this set of guidelines because that would need to be considered in the app’s design. In guideline (e), the developer should consider including the end-to-end security in the risk information presented to the user. These guidelines, we feel, will help the user (in this context, a patient or caregiver) by making them aware just-in-time of any negative consequences of them continuing with recording the interaction with a healthcare professional.

4. The Way Ahead

The topic of privacy in the context of recording PHI is a fascinating one with several dimensions both around the privacy, security, ethics and legal aspects and around what aspects of a patient’s healthcare experience is being recorded. In this paper, we have presented an initial exploration of the literature around a comprehensive look at the privacy issues around recording PHI and presented a set of guidelines for developers for consideration when developing recording

apps. In our future work, we plan to continue exploring the various dimensions around recording and PHI and will explore developing and evaluating technological solutions for the same.

References

- [1] Warren, S. D. and Brandeis, L. D., (1890). The Right to Privacy, *Harvard Law Review*, Vol. 4, No. 5., pp. 193-220.
- [2] Cavoukian, A., Privacy by Design: The 7 Foundational Principles. [Online] Available: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>
- [3] Nolan, B., Ackery, A., & Au, B. (2018). What to do when a patient wants to record a patient-physician interaction in the emergency department. *CJEM*, 20(3), 471-475. doi:10.1017/cem.2017.23
- [4] Stoycheff E, Liu J, Xu K, Wibowo K. Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*. 2019;21(3):602-619. doi:10.1177/1461444818801317
- [5] Government of Canada, Justice, Laws Website, "Privacy Act of Canada (ATIP)," [Online], Available: <https://laws-lois.justice.gc.ca/PDF/P-21.pdf>
- [6] Government of Canada, Justice, Laws Website, "Access to Information Act of Canada (ATIP)," [Online], Available: <https://laws-lois.justice.gc.ca/eng/acts/A-1/index.html>
- [7] Government of Canada, Justice, Laws Website, "Personal Information Protection and Electronic Documents Act of Canada (PIPEDA)," [Online], Available: <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>
- [8] Nova Scotia Legislature, Legislature Website, "Nova Scotia Freedom of Information and Protection of Privacy Act (FOIPOP)," [Online], Available: <https://nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf>
- [9] Nova Scotia Legislature, Legislature Website, "Nova Scotia Personal Health Information Act (PHIA)," [Online], Available: <https://nslegislature.ca/sites/default/files/legc/statutes/personal%20health%20information.pdf>
- [10] Ontario, e-Laws Website, "Ontario Freedom of Information and Protection of Privacy Act (FIPPA)," [Online], Available: <https://www.ontario.ca/laws/statute/90f31>
- [11] Ontario, e-Laws Website, "Ontario Personal Health Information Protection Act (PHIPA)," [Online], Available: <https://www.ontario.ca/laws/statute/04p03>
- [12] Government of Canada, Justice, Laws Website, "Criminal Code of Canada, Part VI Invasion of Privacy," [Online] Available: <https://laws-lois.justice.gc.ca/eng/acts/C-46/>
- [13] Canadian Medical Protective Association. (2017) Smartphone recordings by patients: be prepared, it's happening. *CMPA Perspect.* [Online] Available: <https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2017/smartphone-recordings-by-patients-be-prepared-it-s-happening>
- [14] Oyedokun, T., Donauer, A., Stempien, J., & McKay, S. (2019). Self-documentary in the emergency department: Perspectives on patients recording their own procedures. *CJEM*, 21(3), 384-390. doi:10.1017/cem.2018.423
- [15] Henken, K.R., Jansen, F.W., Klein, J. et al. (2012). Implications of the law on video recording in clinical practice. *Surg Endosc* 26, 2909–2916
- [16] Tsulukidze, M, Durand, M-A, Barr, P. J., Mead, T., Elwyn, G., (2014) Providing recording of clinical consultation to patients – A highly valued but underutilized intervention: A scoping review, *Patient Education and Counseling*, Volume 95, Issue 3, Pages 297-304
- [17] Tsulukidze, M, Grande, S.W, Thompson, R., Rudd, K., Elwyn, G. (2015) Patients Covertly Recording Clinical Encounters: Threat or Opportunity? A Qualitative Analysis of Online Texts. *PLoS ONE* 10(5): e0125824.
- [18] Elwyn, G., Barr, P.J., Grande, S.W. (2015) Patients recording clinical encounters: a path to empowerment? Assessment by mixed methods, *BMJ Open* 2015;5:e008566.
- [19] Lipson-Smith, R., White, F., White, A., Serong, L., Cooper, G., Price-Bell, G., Hyatt, A., Co-Design of a Consultation Audio-Recording Mobile App for People With Cancer: The SecondEars App
- [20] The World Bank, "Mobile cellular subscriptions (per 100 people)," [Online] Available: <https://data.worldbank.org/indicator/IT.CEL.SETS.P2>
- [21] Canary, A., (2020) "The Best Apps to Record Phone Calls" [Online] Available: <https://www.rev.com/blog/best-apps-to-record-phone-calls>
- [22] Canary, A., (2019) "10 Best Voice Recorder Apps for Android" [Online] Available: <https://www.rev.com/blog/best-voice-recorder-apps-for-android>
- [23] Samsung UK, "How do I use the voice recorder app?" [Online] Available: <https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-voice-recorder/>
- [24] Apple Inc., "Making a recording in voice memos on iPhone," [Online] Available: <https://support.apple.com/en-ca/guide/iphone/iph4d2a39a3b/ios>
- [25] Tanner, J., (2013). "Understanding and Buying Digital Voice Recorders," [Online] Available:

<https://www.familysearch.org/blog/en/understanding-buying-digital-voice-recorders/>

[26] Kessels, R. P. C. (2003). Patients' memory for medical information. *Journal of the Royal Society of Medicine*, 96, 219–222. doi:10.1258/jrsm.96.5.219

[27] Jackman, T. (2015, June 23) “Anesthesiologist trashes sedated patient –and it ends up costing her”. *Washington Post*. [Online] Available: https://www.washingtonpost.com/local/anesthesiologist-trashes-sedated-patient-jury-orders-her-to-pay-500000/2015/06/23/cae05c00-18f3-11e5-ab92-c75ae6ab94b5_story.html