Team 29 Legal Issues Report

Our team worked in collaboration with NTTData (Nippon Telegraph and Telephone) and Great Ormond Street Hospital (GOSH) to provide a wireless sensor suite for performing sleep studies. We modified NTTData's Hitoe t-shirt, which is a t-shirt with embedded heart activity and posture sensors, to send its data to a cloud server where the data can then be displayed on a web portal. I will discuss the legal issues associated with this project including the contractual deliverables, potential liabilities of the system, intellectual property issues, and data privacy concerns.

The deliverables of this project include a modified Hitoe Android App, a cloud infrastructure deployed on Microsoft Azure, and a web portal. These separate components must be integrated into a working system and tested thoroughly before handing them over to our client, NTTData. It was agreed upon between our team, NTTData, and GOSH that the system would not be expected to be ready for use in a clinical setting but would be a proof-of-concept that the data from the Hitoe t-shirt can be stored and retrieved from a database in real time. Thus, the system produced was expected to be rough and in need of additional development before deployment. The Android app would be developed by our mobile developer, Mariam, the cloud infrastructure by our back-end developer, Vijey, and the web portal by our front-end developer, Abhinath. These roles were agreed upon in the research phase before the start of development. The components are to be delivered by 22 March 2018.

This system will eventually be deployed in a clinical setting and thus has some key liabilities. Firstly, the accuracy of the data provided by the Hitoe is the responsibility of NTTData. Any inaccuracies in the data which lead to a misdiagnosis for a patient could be attributed to NTTData. Secondly, our system will have to ensure that all data is stored in the database with no data loss. Loss of data can lead to the invalidation of a sleep study resulting in wasted resources. NTTData could be held accountable by the hospital for these losses. Lastly, NTTData could be held accountable for the security of patient data stored in the system. Any security breach caused by a flaw in the system's security could be the fault of NTTData. It is important to note that while there are many potential liabilities, whether NTTData will be held accountable depends entirely on the licenses and agreements on the software and the contract made between NTTData and the hospital using the product.

Everything produced in this project inclusive of source code, videos and websites are the intellectual property of NTTData as per the contract between NTTData and UCL. With regards to licenses, the only proprietary software used in this project is the Hitoe SDK which is the copyright of NTT Docomo, a sister company of NTTData. Since the code produced is owned by NTT Data, there are no licensing issues with using the proprietary software in our code. The remaining code was produced using open-source software namely PHP, Apache, MySQL, Chart.js, HTML5 and JavaScript. These technologies are licensed under various open-source licenses. This means that we are free to modify and use the code of these technologies. None of these licenses have "copyleft" clauses which would require any product made using them to be open-source too. This means there are no licensing issues, and NTTData is free to commercialise the product as they see fit.

The software will have to be licensed to protect the intellectual property and to prevent security breaches. Our recommendation for NTTData would be to license the software and not to distribute the source code. The software we have produced in this project is built specifically for the Hitoe and uses the proprietary Hitoe SDK heavily. There would be little benefit to the community to make this software open-source since they would not have access to the Hitoe SDK. Furthermore, there may be security issues with allowing the software used for a clinical device to be open-source as malicious individuals might choose to exploit security flaws in the software. Thus, the software produced from this project should be licensed and copyrighted by NTTData and its source code should be protected.

Our system stores patient medical information and will have to secure the data in accordance with medical guidelines to protect patient confidentiality [1]. Currently, the web portal can only be accessed with a username and password. While the database administration is protected by two layers of username and passwords. These are steps in the right direction, however they are not enough to comply with the requirements of the medical guidelines. To fully comply with the guidelines, doctors should only be able to access the data of patients that they oversee and the system should delete data after it is no longer required by the hospital.

In conclusion, this project has multiple components which had to be delivered including an Android app, a cloud infrastructure and a web portal. The intellectual property of this project belongs wholly to NTTData and they are free to license this software commercially without breaching the licenses of the technologies used. NTTData should not distribute the source code of this system to prevent potential security breaches. To comply with medical guidelines on patient data privacy, NTTData should work on implementing additional privacy features such as preventing doctors from viewing patient data they are not supposed to be able to see and deleting unused patient data.

References

[1] Head of Corporate Information Guidance, National Health Sercvice England, "NHS England Information Security Policy," June 2016. [Online]. Available: https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v3-1.pdf. [Accessed 20 March 2018].