Bluetooth vs. Wifi Regulation Research

Haeryn Kim, Lizbeth Leapo, and Deepthi Nacharaju

What is considered Protected Health Information?
According to the HIPAA Administrative Simplification regulations by the U.S. Department of Health and Human Services, the term *health information* refers to "any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." *Protected health information*, on one hand, means **"**individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium." (HIPAA Simplification)

What are areas of protected health information that is relevant to our product that the hospital currently reserves the right to use or disclose, under patient consent?
The hospital currently can use protected health information for healthcare operations, which include "reviewing and improving the quality, efficiency and cost of care that we provide to you and other patients." (Duke Health, Notice of Privacy Practices)

What are the current privacy practices at Duke University Hospital?
On Duke University Health System websites, they use analytics tools and other third party technologies, such as Google Analytics or DoubleClick Cookies to collect non-individual information in the form of various usage and user metrics when the user employs these services. The mentioned information include "cookies, IP addresses, device and software identifiers, referring and exit URLs, onsite behavior and usage information, feature use metrics and statistics, usage and purchase history, MAC Address, mobile unique device ID, geo-location, demographic and interest data, and other similar information." (Duke Health, Website Privacy Policy)

They also use a WiFi network as is secured under settings required by the Code of Federal Regulations (CFR) Title 45, Part 164, Subpart C. The CFR splits the requirements into three categories: administrative (pertaining to the configuration of the wireless LAN), physical (ex. security-lock secured access points), and technical (separation of traffic, WPA2 and PSK encryption). Should our device transmit information using WiFi, encryption should be taken care of by the hospital's system; but multiple devices use the same WiFi network at the hospital.

How is information transmitted in Bluetooth?
Bluetooth networking transmits data via low-power radio waves. It communicates on a frequency of 2.45 gigahertz. Bluetooth systems can create a personal-area network, or a piconet, that may fill a room, e.g. the patient room. Once a piconet is established, the connected devices randomly hop frequencies in unison (1600 hops/sec) so they stay in touch with one

another and avoid other Bluetooth connections that may be operating in the same room. (Franklin and Layton)

What kind of individually identifiable data are generated by Bluetooth?
In the case of our system, the signal detector (the bedside sensor) that detects patient input, that reads and transmits boolean data (True if a patient's hand is near the sensor for more than five seconds) to a signal receiver (a servo motor) unit that is in the same room, within the range of Bluetooth. This data is not individually identifiable of the patient.

How is information transmitted in Wifi?
Data is transmitted over Wifi using the connection to the internet. Usually, there is a central node (a router) that acts as the interface between wired and wireless connections and manages communication between devices. This device also exchanges data packets between devices. It is called an Access Point (AP) or a router. A client, a mobile phone, laptop or workstation computer, connects to the AP. The client sends data packages to a router that is modulated using Orthogonal Frequency Division Modulation. These data packages are tagged with the physical address of the receiving device (MAC address) and it is sent to the atmosphere of the Mac ID of receiver. All of the devices in the range of the AP can capture this package, but the only device with the specified Mac ID will be able to retrieve and process the data. (Syed)

What kind of individually identifiable data are generated by Wifi?
Similarly to Bluetooth, the data being transmitted is agnostic to the user so there is no individually identifiable data transmitted through Wifi between the devices. However, there necessarily will be information transmitted through the hospital Wifi and characteristic to any requests made through the internet, an exposed Mac/IP address of the devices. However, multiple devices require connection to the same network and it would be unlikely that our device can be configured to a separate network traffic. It would be also harder to troubleshoot security, since our developers would have limited access to any information pertaining the Duke Health WiFi configuration.

Could anything mentioned have possibility of being considered private patient record?
No. The two devices that comprise our system will transmit signal from an IR sensor, that generates information agnostic to the user, to a signal receiver that does not either interface with Bluetooth or Wifi to interact with a remote controller button. This interaction is purely mechanical.

Why is Bluetooth more apt for our purposes?
In consideration of the attributes that are inherent in wireless connections, such as usability, power, distance, data rates, and coexistence, Bluetooth is the ideal option as a wireless connection module for the degree of performance necessary for our device. It consumes the least power of all of the networked technologies. It typically requires fractions of the power of IEEE 802.11b solutions. Typical PDA implementations yield 6–10 hours of usage compared with 2–4 hours for 802.11 solutions using the same batteries. (Saltzstein) With Bluetooth, no IP

addressing is involved, so it is relatively quick and easy to set up small networks of devices. It also has the necessary security features to comply with HIPAA requirements for patient data. It is cableless (a high priority in our design specifications matrix), has high connectivity within individual patient rooms, security that provides access control and software encryption options, is reliable based on resistance to ambient radio frequency noise, and has a low level of interference with other technologies.

References

Duke Health. Notice of Privacy Practices. https://www.dukehealth.org/privacy. Web. 2 Dec. 2018.

Duke Health. Website Privacy Policy. https://www.dukehealth.org/privacy. Web. 2 Dec. 2018.
Franklin, Curt and Layton, Julia. How Bluetooth Works.
https://electronics.howstuffworks.com/bluetooth2.htm. Web. 2 Dec. 2018.

The Health Insurance Portability and Accountability Act Administrative Simplification Part 164 Subpart C. Web. 4 Dec. 2018.

Public Welfare, 45 C.F.R. § 164.C (2012).

Saltzstein, William E. Bluetooth and Beyond: Wireless Options for Medical Devices. Medical Device and Diagnostic Industry.
https://www.secplicity.org/2015/08/31/hipaa-compliant-wi-fi-what-you-need-to-know/. Web. 6 Dec 2018.

Syed, Amal. How does data get transmitted via Wifi? Quora.
https://www.quora.com/How-does-data-get-transferred-via-WiFi. Web. 5 Dec. 2018.