A.1 Interview protocol – Healthcare Delivery Organizations

A.1.1 Participant background

1. What is your role here at *(organisation)*?
   (a) For how many years are you already working in this position?
2. What is your role here with respect to medical devices?
   (a) What type of medical device classes are you responsible for?
3. How many medical devices are there in your organization?
4. How many medical devices in your organization are connected (i.e., to networks)?
   (a) (If applicable to role) And how many connected medical devices in total are you responsible for?
5. How do you keep track of and manage these connected medical devices?
   (a) Does this work out well from your perspective?
   (b) (*If it's not perfect*; What would help you to improve the management of connected medical devices?

A.1.2 Patching process

1. What percentage of the software updates you install on connected medical devices would you estimate are **security** updates? (i.e., they close vulnerabilities in some software or hardware component)
2. Let's say a security update has to be installed on a connected medical device. Can you walk me through the process of how this updating works at your organization?
3. (*If questions 5 - 8 have already been answered before, omit accordingly.*)
4. How is it decided which devices need to be updated and when, and who decides?
5. How do you learn about available updates?
6. Who do you typically interact with during this process? What is their role in this?
7. Are updates tested before they are installed, and if yes, how?
8. Do you have any certifications to be able to install updates on connected medical devices?
9. How often do you have to be (re-)certified?
10. Now I would like to ask you some questions about the last three times you installed a security update on a connected medical devices. What were the last three medical devices you were involved in patching?
11. For each of them, can you tell us...:
    (a) What kind of medical device was it?
    (b) From which manufacturer is the device?
    (c) When did you install the update on this device?
    (d) How did you learn about the need to update?
    (e) How often do you usually install updates on this device?
    (f) How are updates installed on this device? (e.g. remote? manual? by manufacturer technician? Installation steps?)
    (g) How is the device connected to the rest of the organization?
    (h) What kind of issue did the security update fix, if you know?
    (i) What was the time span between the *release* of the update to the *installation*, if you know?
12. What are the biggest challenges you face when it comes to keeping connected medical devices up-to-date?
13. How do you handle these challenges?
14. *If the following topics have not been mentioned previously:*
    (a) How do you handle connected medical devices that don't receive software updates anymore and stay in service?
    (b) How do you deal with downtime, when the device is updated and not available for medical use?
    (c) Were there situations when the installation of an update led to problems with the device's performance? If yes, what do you do in such cases?
15. Are there any security risks you are concerned about when it comes to connected medical devices at your organization?

A.1.3 Regulatory factors

1. Which national and international regulations do you follow when dealing with connected medical devices, if any?
2. How do these regulations effect the software updating process within your organization, if at all?

A.1.4 Hospitals' stance towards manufacturers

1. How is the manufacturer of the medical device involved in the updating and patching process of medical devices?
2. In your experience, do medical device manufacturers meet their responsibilities in keeping connected medical devices secure at your organization?

A.1.5 Closing question:

1. Thank you very much for taking he time to talk to us. Do you have any closing remarks or things you would like to mention?
2. Can you recommend a colleague at your organization or at another one, who works in a similar position (is involved in patching) and could participate in our study?

A.2 Interview protocol – Manufacturers

A.2.1 Participant background

1. What is your role here at *(organisation)*?
    (a) For how many years are you already working in this position?
2. What kind of medical device products are you dealing with in your work?

A.2.2 Patching Medical Devices

1. How often do you release security updates for your connected medical device products?
    (a) *(Potential follow-up questions;)*
    (b) Is this different for different devices? Why?
    (c) What percentage of the software updates you release for your connected medical device products would you estimate are **security** updates?
    (d) Are security updates bundled with other kinds of software updates, such as performance or feature updates? If yes, why?
2. How is it decided if and when you release a security update for your connected medical device products?
    (a) *(Potential follow-up questions;)*
    (b) Which factors do you consider in this decision?
    (c) Which actors are involved in this decision? (e.g., (Software) vendors, authorities, customers)?
    (d) What kind of risks do you want to protect your products against?
    (e) How are such risks assessed?
    (f) How do regulations affect the decision if and when to patch?
    (g) In your experience, what are the biggest challenges when it comes to risk assessment and deciding about security patching?
3. Once it is decided to release a security update for your connected medical device products, how does this update reach the devices at your customers' sites?
    (a) *(Potential follow-up questions;)*
    (b) What are the different processes to do so?
    (c) What are the different processes' prevalence? i.e., Which patching process is most and least common?
    (d) To what degree can customers decide on how to install security updates?
    (e) How are customers notified about available security updates?
    (f) If technicians are sent to install security updates, how often does this happen?
    (g) Are there differences between countries how this process works?
    (h) What are you observing how these patching processes work out in practice with your customers?
    (i) In your experience, what are the biggest challenges when it comes to deploying security updates to medical devices at your customers' sites?
4. Do you keep track of your connected medical device products in circulation and their software versions? If yes, how?
    (a) *(Potential follow-up questions;)*
    (b) If you cannot keep track, how do you go about updating them?
    (c) Do you have means to know if the security update has been installed or not?
    (d) In your experience, what are the biggest challenges when it comes to tracking the software versions and updates of your medical devices at your customers' sites?

A.2.3 Closing question:

1. Thank you very much for taking the time to talk to us. Do you have any closing remarks or things you would like to mention?