Digital Assistants: Alexa can handle patient information – what does that mean for privacy?

Lorene Novakowski
February 7, 2020
Alexa and HIPAA

• Amazon Alexa devices achieved HIPAA compliance
• In order to qualify as a covered entity under HIPAA, Amazon entered into a business associate agreement with a covered entity, whereby it promised to abide by the same regulations as a covered entity and only provide public health information to covered entities for their explicit use
Alexa and HIPAA cont’d

- Alexa needed to update its software to a standard that it could transmit private patient information safely and responsibly.
In order to comply, Amazon had to prove that it had implemented safeguards to prevent personal health information from being accessed from unauthorized individuals, which include end-to-end encryption to prevent interception of data.
Alexa and HIPAA cont’d

• Amazon also had to show that the device could only accept commands from an authorized individual.

• For example, physicians could dictate notes or send an order to the pharmacy but others could not.
Alexa and HIPAA cont’d

- Ongoing considerations in light of the types of health care offerings being considered, such as conversational diagnosis, contextual care plans, detection of in-home emergencies, are how to transmit sensitive information privately without broadcasting to a roomful of people, how to decipher patient data, other data
What about Canada?

- Patchwork health privacy legislation across Canada, in all but British Columbia
- Generally, covers information about diagnostic treatment and care information, or information relating to the physical or mental health of the individual or the healthcare of the individual
What about Canada, cont’d

- Health information or personal health information can be transmitted within the “circle of care” without express consent of the patient.
- Would the app provider be a custodian or an agent or affiliate?
- What about Amazon – would it be an agent and required to comply with health privacy legislation?
Requirements to Protect Information

• In Ontario, in Orders HO-004 and HO-007, any personal health information stored on mobile devices must be strongly encrypted.

• Question: whether the encryption to achieve HIPAA compliance meets the standard?

• Encryption would seem necessary to comply with security requirements in Canada.
What about the Other People in the Room?

• Would the end user (the patient) be able to complain against the service provider if the patient allowed other persons in their room to hear incoming information about treatment, etc.
What about the Other People in the Room?

- Would privacy policy of service provider need to deal with these issues?
  - Livongo, Express Scripts privacy policies do not
  - PIPEDA Case Summary #2004-270
Where would the Data be Stored?

- Alexa records conversations to Amazon’s cloud
- In British Columbia, if FIPPA applied to the health information, would it need to be stored in Canada (or would the new exception to FIPPA apply)?
- Ontario PHIPA requires express consent to disclose PHI outside Ontario
Security Issues

• Would the digital assistant be safer than the human assistant?

• Examples:
  • December 2019 – Lifelabs hack
  • October 2019 – Shuswap Hospital delivered another patient’s medical information in the mail
Security Issues cont’d

• Examples, cont’d:
  • December 2019 – Kamloops detox centre gives personal belongings of one resident to the wrong resident who was checking out (cell phone, credit cards, ID, bank cards)
  • April 2019 – St. Boniface Hospital (Winnipeg) reported 38 patient records had been viewed inappropriately by employees
Security Issues cont’d

- October 2018 – Alberta Health Services notifies 178 patients that their health information was inappropriately accessed by a former administrative employee.
Conclusion

- Digital assistance with the type of strongly encrypted software to protect against unauthorized intrusion may allow for introduction of technology to make things easier for patients
Conclusion cont’d

• Examples:
  • Diseases like diabetes that require constant monitoring, which could be done remotely
  • Avoiding follow-up appointments for those receiving cancer treatment or who had surgery
  • Assisting the elderly or those who are not mobile by allowing access to medical information without having to travel
Conclusion, cont’d

• The benefits of tools like Alexa in the healthcare industry should not be shunned because of the privacy considerations, but privacy needs to be built into the design
Conclusion, cont’d

• Canadian regulators should scrutinize the HIPPA compliance approach and do their own investigation as to whether or not Amazon’s tools are privacy compliant for Canada.
Lorene Novakowski

- Partner
- +1 604 631 3216
- lnovakowski@fasken.com
FASKEN