

TeleAudiology: Privacy and Practicality

Privacy, Solutions, and Examples
Bill Campbell, Audiologist, Ontario Canada
Linda Hazard, Ed.D., Virginia

1

Acknowledgements

- Dr. Danielle Glista, Western University.
- Dr. Salima Jiwani, Audiosense
- Dr. Jacob Shelley, Western University, Health Ethics, Law, and Policy Lab.

2

Getting to a Comfort Zone

- Why privacy and confidentiality?
- Privacy legislation is incomprehensible.
- Understanding risk, responsibilities, and liability.
- A change in the wind.
 - Who's responsible for what?
- Practical solutions. How to...
 - Videoconference solutions.
 - Real world counseling experience.

3

Why?

- What **data** might be transmitted during eAudiology?
- Personal Identifying Information (PII)
 - In the US, PII is protected by multiple federal and state regulations.
 - Any data or information that may be used to distinguish or trace a person's identity
- Health Information (HIPAA)
 - Audiometric data
 - When eAudiology is used for screening or assessment.
 - Hearing Aid data
 - When hearing aid adjustments are performed.

4

Why?

- What **visual or audio** might be transmitted during eAudiology?
 - Patient identifying information
 - Patient's image.
 - Spoke site (patient) environment.
 - Case history information.
 - Patient intervention information.
 - Tinnitus counseling.
 - Auditory rehab.
 - Vestibular counseling.

5

Security-Cyberattack

University of Vermont Health Network

- Hospitals impacted in Vermont and upstate New York
- Ransomware
- All systems on backup
- October 28th-November 23rd (no access to electronic medical record)
- Surgeries, office visits and diagnostic evaluations cancelled

6

The Privacy Pit



- **HIPAA: US law, self-certification (1996)**
 - Federal law governing privacy and security of Personal Health Information for the health industry. State laws exist governing PHI as well.
 - Requires administrative, physical, and technical safeguards for PHI.
- **GDPR: General Data Protection Regulation (EU member states)**
 - Similar to HIPAA, and outlines accountability and responsibility for collected data.
- **Safe Harbor (Patriot Act, NSA, Homeland Security...)**
 - Governs storage and accidental disclosure or loss of personal information.
- **Privacy Act**
 - Allows a person to know why, how, and where information is collected, used, and stored and to whom it may be disclosed.

7

Spirit vs Letter

- Existing privacy regulations, policies, and guidelines are generally hopelessly complex and outdated.
- It is not feasible or reasonable for clinicians to have a full legal understanding of relevant privacy regulations or of supplier policy.
- “The critical question is whether [the clinician and/or] institution has taken reasonable steps to protect the privacy and security of records in it’s custody and control” (OIPC).
- Clinicians must act in good faith that the tools we are using and the guidance we’ve been given is appropriate for the job we are doing.

8

If We Don’t Know, Who Does?

- Who can we count on to interpret and advise us on the applicable aspects of privacy legislation
 - Be as educated as you can. Apply that knowledge with common sense.
 - Your college or regulatory body is a key contact.
 - Your institution or agency.
 - Talk to a lawyer (consider the cost involved).

9

Mitigation

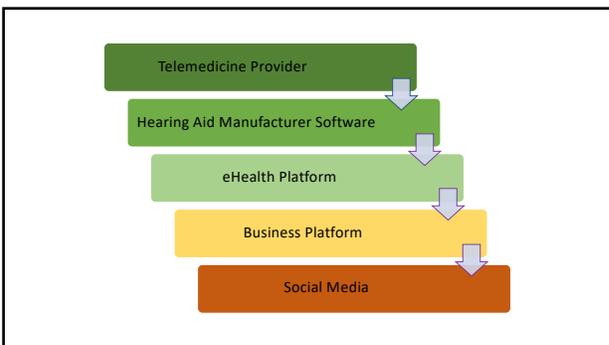
- All data collected should be for a specific purpose.
 - DON’T collect or retain any information that you don’t need.
- Delete data that is no longer needed.
 - Don’t keep records longer than necessary.
- Don’t record or store data in an unsecure place!
 - Use a unique identifier where possible.
 - Encryption
- Review data for accuracy.
 - Review data with the client.

10

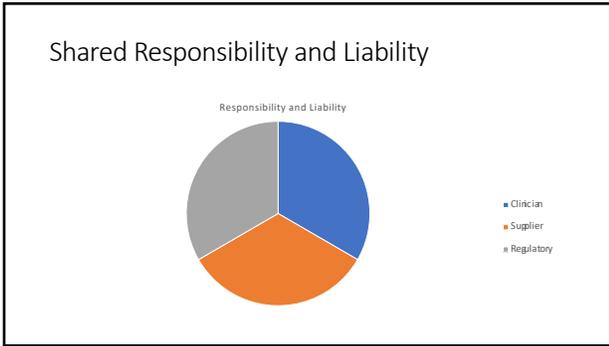
Mitigation

- Select and maintain a provider based on:
 - Obviously; no social media oriented platforms
 - Choose a solution based on the security hierarchy
 - Advertised compliancy
 - Privacy policy/statement
 - Regulatory body approval or recommendation
 - Experience

11



12



13



14



15



16

What's a BAA?

- Business Associate Agreement.
 - This specifies the responsibilities of each party involved in the handling of patient PHI and PII.
 - Typically, do not expire once signed.
- You should have a BAA with any party that stores, handles, accesses PHI. This would include client management software solutions, hearing aid manufacturers, video/audio conference solutions....

17

Practical Solutions for Videoconference

- Private eHealth Provider Examples
 - Doxy.me: Website claims HIPAA, GDPR, PHIPA/PIPEDA compliance. BAA included. No privacy/security differences between free and paid.
 - TheraPlatform: US based videoconference solution designed for SLP's and other similar health professionals. HIPAA compliant with BAA included. Pricing for single providers, with varying degrees of scheduling and billing features. Tech support and BAA. Secure chat and messaging. Online system monitoring.
 - Cisco Webex: US based, business oriented with eHealth component. HIPAA compliant. BAA available. Global hosting. Transcripts available**
 - Zoom (and Zoom Healthcare). Zoom has a statement indicating HIPAA compliance, and has a BAA option.

18

BUT.....

- Technology and providers change quickly.
- What was current and applicable a few years ago has changed.
- Be prepared for change. Either internal or external.

19

Hearing Aid Manufacturer

- All current manufacturers offer some sort of remote connection to later model devices.
- All major manufacturers offer secure videoconference and/or chat as well.
- Data transferred through these platforms is GDPR compliant.
- Bottom line: Use of hearing aid manufacturers software to connect to and interact with a patient can be considered as “acting in good faith”.
- Whenever possible, synch new hearing aids to remote options even if the patient may not use it.

20

Two Birds with One Stone

- There can be confusion in finding a videoconference solution.
- What about use of a manufacturers solution for all aspects of eAudiology?
 - The embedded videoconference solution could be used regardless of the client’s hearing aid brand and age.
 - This component of manufacturer software will continue to expand in future.
 - Patient (spoke site) must have appropriate technology.
 - Spoke site must be secure, to the degree that the patient understands and consents to any risks to confidentiality.

21

Other options

- Online or app based hearing assessment
 - Mimi
 - uHear
- Caveat: Where is data stored, how is it used/accessed by the app developer?

22

Resources

- NCHAM Learning Community.
- NCHAM: The Impact of Privacy Regulations, White Paper
- American Academy of Audiology Practice Management: https://www.audiology.org/practice_management/compliance/compliance
- IAPP.org https://iapp.org/media/pdf/resource_center/Comparative_Table_of_Personal_Information_Protection_Laws_English.pdf

23

Resources

- Oticon RemoteCare
 - <https://www.oticon.ca/professionals/training-and-fitting/training/webinars>
- Phonak eSolutions
 - www.phonaklearning.ca/esolutions
 - Daily live session at 12 pm EST and Wed. at 3 pm EST
- Starkey Hearing Care Anywhere
 - https://starkeywebex.com/webex/sites/starkey/recording/play/5c59cb081764cc10674a13285d94101a11m_source=00102136900anibw0attendee001m_campaign=86630547-407a1e-41W2A165-0024-12-18-108-31&form_messaging=enhanced&form_termid=1e1d52948d47-40421092374211741100000
- Sivantos Telecare 3.0
 - https://www.aspireportal.ca/v/vs0files/trainingwebinars/SigniaTeleCare.mp4?utm_source=mail
- Al-Abri et al, 2016. The accuracy of IOS device based uHear as a screening tool for hearing loss: A preliminary study from the Middle East. Oman Medical Journal,31(2); 142-145

24

Questions?

- bill@superiorhearing.ca
- linda.hazard@partner.Vermont.gov