Project for chapter1

Idea:

Hi, I am Simi. I am 13 and I recently got diagnosed with dyslexia.
In the process of doing the dyslexia test and finding a therapist, I got an idea that could only be done with the privacy concepts we learned in this course.
When I first met my therapist we didn't know what exactly my weaknesses are therefore it was hard to tackle them and even my 4-hour test couldn't do that. The idea is that the therapist adds the learning process(what task you did, how good you were) and the hospitals would add the test scores about every 3 years when you take the test. And when a therapist gets a new kid she can check with the AI module which treatment would work. And this hasn't happened jet since it would be a huge privacy problem to share this data with every therapist. You would give your test score and get an answer without revealing the data.

value:

this would help so many dyslexics and with this technology, it could also help other learning disabilities and mental health issues as well as their doctors and therapists.

comparing to existing technologies:

I found: https://www.cambridgebrainsciences.com/
which is the first step of having the dyslexia test in a digital format.
My service would further secure user data and preventing data misuse with privacy technologies (since the data set would not be revealed to anyone)
and also give an effective therapy plan based on available data(giving further features and usabilities).

Audience + use case

the audience would be hospitals sending their tests and then be able to see how their dyslexia rates are, therapist sending the process and also checking it for herself and the kids and parents to check their progress. for safety reasons(explained below) my service will use privacy technology(also explained below) and the kids and parents will save time, effort, and in some places money(->therapy plan).

Information Flows:

information flow1:
hospitals send the test
(input privacy-> multiple people will create a flow without letting the other person letting know what other peoples flow would be)
this will solve the copy problem, which means that people would not be able to duplicate the data set. (solving the copy problem)

(input verification->
allows you to verify the integrity and origin of a flow of information without
revealing additional information right, you would check that this information has not been changed and that it is from a trustable source(hospitals))
this will ensure that no false data will come so that the ai algorithm will give the most accurate response to the input. (allows you to verify the integrity and origin of a flow)

flow governance: if the hospitals would want to change anything to the information flow they would have to
ask for the approval of the patient, solving the recursive enforcement problem(no one will have the upper hand over the data set.)

information flow2:
therapists send weekly updates on the progress (input privacy-> multiple people will create a flow without letting the other person letting know what other peoples flow would be)
this will solve the copy problem, which means that people would not be able to duplicate the data set. (solving the copy problem)

(input verification->
allows you to verify the integrity and origin of a flow of information without
revealing additional information right, you would check that this information has not been changed and that it is from a trustable source(therapist))
this will ensure that no false data will come so that the ai algorithm will give the most accurate response to the input. (allows you to verify the integrity and origin of a flow)

flow governance: if the therapists would want to change anything to the information flow they would have to
ask for the approval of the patient, solving the recursive enforcement problem(no one will have the upper hand over the data set.)

flow3:
the AI module gives an appropriate response to flow 1 based on current data about what the correct treatment would be. (this would need output privacy -> is the ability to filter a flow of information so that only the individual bit that you wanted to share is is shared without accidentally revealing anything else)
This solves the bundling problem.

Output verification-> this privacy technology would also be needed since you would have to verify if the output is correct and if the ai module is fair. This is important since you need the module to give you the correct output otherwise the therapy plan would be faulty and it would be done by having an other algorithim checking if this outpout is the one we want.

Privacy
For using Privacy tools- I suggest Encryption tools. For Data in Transit- we use TLS 1.3 or higher. And for data at rest- any commercial encryption tool.
For privacy tools, I would use homomorphic encryption(to encrypt the patients data). Since multiple hospitals would send their input and then the ai module would predict the best therapy plan. So nobody, not even the module would see your real data, since it would be encrypted first.

1.For input verification I will apply digital signatures, wich is is a mathematical scheme for verifying the authenticity of digital messages or documents.

2.For output privacy I will use differential privacy by applying random noise according to the privacy budget epsilon on my input data

3. For flow governance I will share the ownership of a number(data) across the people _> hospitals and patients.
I will govern the information flow by using secure multi-party computation.

you won't have to deal with the privacy transparency trade-off:)