Andrew Yorra
andrew@yorra.net
(503) 395-7171

March 1st, 2023

Committee on Health Care
Oregon State Senate
RE: SB 303 Additional Comments

Dear Senators,

In reviewing submitted testimony, it appears there are some misunderstandings and factual inaccuracies that should be addressed. Additionally, I wanted to share some events in the past two days that demonstrate the real risk this project poses to Oregonians' privacy and safety. This letter supplements my previously submitted testimony that also provides my background as a cybersecurity professional and attorney.

We heard testimony that only OHA will have the individualized data and OHSU will only have aggregated data. We also heard conflicting testimony that OHA will be doing the de-identifying of the data while others saying service centers will.

Before addressing these conflicting positions, we need to ensure policymakers and the public understand data categories as intended by scientists doing the research and lawyers writing the laws. Personally Identifiable data is an individual record that can be connected to a specific individual. De-identified data is when the identifiable data of the individual record is removed or transformed, sometimes permanently but in most cases, able to be re-identified by those who did the de-identification (or a hacker on their network). Aggregated data are solely summary numbers that are based on the individual data, but contain no individualized records (neither de-identified or personally identifiable).

Based on the bill's plain language, discussions with its backers and OHSU, and Senators' public statements, it appears the intent is for service centers to provide all individualized (de-identified) records to OHA who would share all those records with OHSU, which would share them with its research partners that range from regional healthcare organizations to clinical researchers in private practice. Healing Advocacy Fund claims in their letter that the bill intends that service centers and not OHA do the data aggregation of the individualized de-identified data. But that contradicts the bill's plain language that requires reporting to OHA of extensive individualized data, such as a client's race, ethnicity, veteran status, the reasons they sought service, adverse experiences, etc. OHSU has also said that they require individualized data for their research and aggregated data is insufficient. This means that the full individual (de-identified) data set will be provided to OHA and OHSU and accessible to OHSU's academic and commercial research partners.

This means that SB 303 will mandate massive collection of individualized de-identified (but potentially identifiable) data on nearly everyone who receives psilocybin services. It's also important to recognize this data will also contain individualized **personally identifiable** information of every facilitator and service center operator without any opt-out.

Andrew Yorra
andrew@yorra.net
(503) 395-7171

These databases, if re-identified, could expose thousands of Oregonians' sensitive health records including details about their mental health, where and when they took psilocybin, and much more. All of which are still federal crimes.

In the twenty four hours since the committee meeting, the US Marshall service announced it had been breached and a ransomware attacker seized a trove of sensitive data, DISH announced it had been breached and customer information may have been leaked, and the nation's leader on cybersecurity raised an alarm that US companies aren't doing enough to protect their applications from data breaches. Leading cybersecurity researcher Sonatype reports that cyberattacks have increased 742% annually.

Securing a project with this level of sensitive data across and this many actors involved will cost millions to build and millions more to operate safely and securely. And a data breach could be catastrophic for Oregonians, and the psilocybin program. This is too dangerous and too expensive, and as OHA pointed out in its comments, it will likely discourage and not promote equitable access.

The far better approach is to let OHSU and service centers work together directly on a voluntary basis to conduct research on willing participants and pair that with readily available public data like 911 calls, polling and other commonly used research techniques. Oregonians shouldn't have to risk their privacy and data security to receive psilocybin services. Mandated data collection is not required for thorough and valuable scientific research to measure this program's efficacy.

Please let me know if you have questions or wish to discuss. I'm fully committed to working with this committee and OHSU to find a path forward that advances research without putting Oregonians' data at risk.

Regards,

Andrew Yorra