Digital Frontier Alliance

My Data. My Dignity. My Voice.
Data Dignity Pledge

As an organization (or individual clinician) providing behavioral health services – including but not limited to managed care oversight, inpatient or outpatient therapy, community supports, autism, crisis, residential, and substance use disorder treatment – to individuals enrolled in Michigan Medicaid or public substance use disorder programs,

_____ is committed to the protection of Recipient Rights as mandated by the Michigan Mental Health Code (PA 258 of 1974) and recognizes that:

- "Behavioral Health Data" constitutes the most sensitive category of personal information, reflecting the lived experience, dignity, and private struggles of our community members; and
- Every individual has the right to privacy, dignity, and informed consent regarding how their behavioral health information is used, including the right to understand what data exists about them, who can access it, and how it is protected; and
- The evolution of digital technologies, electronic health records, artificial intelligence (AI), and data sharing platforms has created new and complex risks to the privacy of persons served, including gaps in federal and state law that may allow third party data brokers or commercial entities to access, analyze, or monetize behavioral health information without the individual's full understanding or meaningful consent; and
- Protecting the privacy and dignity of persons served is a foundational obligation of the public behavioral health system and that emerging technologies require proactive safeguards, transparency, and clear ethical standards that go beyond minimum legal requirements,

_____ pledges to adopt and implement, through its policies, contracts, Board of Directors' resolutions, and any other appropriate governance or operational mechanisms., the following priorities:

Recognize that Data is a Protected Right: Recipient data is a public health asset and the personal property of the individual; it shall not be leveraged to benefit commercial interests, including profit or "data-sharing credits." Behavioral health data is a protected right, not a commodity.

Implement a Sanctuary Standard of "Meaningful Consent:" All data sharing and privacy disclosures must be presented in plain language, accessible to individuals receiving services. Consent for 3rd-party data sharing must be an active, informed "Opt-In," and refusal to be tracked shall never result in a denial or degradation of care. No recipient shall be "auto-enrolled" into a data-sharing pool. Every individual who consents to enroll must also be provided with a meaningful "Opt-Out" mechanism that is easy to understand and execute at any time.

Reject Extractive Platforms: Any "integrated data" partnerships that require the monetization of recipient profiles as a condition of participation or service shall be rejected.

Prohibit Unsecured Website Tracking: Organizations shall ensure that any third-party marketing tags (Google, Meta, etc.) are removed from or configured on websites to block the transmission of metadata or search intent to commercial servers. Any tracking must be fully scrubbed of personally identifying information (PII) or protected health information (PHI) before transmission.

Define Privacy Zones: Oppose the deployment of intrusive "geofencing" or physical trackers using wi-fi or Bluetooth proximity beacons in the vicinity of outpatient service clinics, non-restrictive program sites, and administrative offices to ensure recipients can access care without being logged by non-consensual surveillance mechanisms.

Reject Broad Data-Sharing Agreements: Prohibit broad or "blanket" data-sharing agreements, especially with private or commercial entities. Each agreement must list the specific data elements to be shared; vague "catch-all" terms (e.g., "all relevant clinical data") are not allowed. Data may be used only for the stated clinical or administrative purpose. Any secondary use (e.g., for product development, AI training, or commercial profiling) is a breach of contract. Each agreement must include a data destruction date and a certified secure deletion process.

Uphold the Spirit of Data Privacy Laws: As technology evolves—especially with AI—new loopholes in privacy and protection laws will keep emerging. The practices and technologies named in this Data Dignity Pledge do not cover every possible loophole. Even so, the public system is responsible for finding and closing – not exploiting – any loopholes that could expose the sensitive information of people receiving services.

Commit to Ongoing Transparency: Provide an annual audit and attestation that these – and other standards as the need evolves – are being met.

The public behavioral health system has long demonstrated a commitment to ethical stewardship of sensitive information, local accountability, and community-based governance, all of which are essential to maintaining trust and ensuring that individuals feel safe seeking care. This pledge reinforces this long-standing commitment.

Adopted by _____ this _____.

A Behavioral Health Workforce Pledge follows on p. 3

Digital Frontier Alliance

Behavioral Health Workforce Pledge

The dignity of our workforce is inseparable from the dignity of our recipients. _____ pledges to its staff, particularly those with disabilities and exceptional needs, that it shall not:

- Track Behavioral Metadata: We will not use "keystroke logging," "attention tracking," or "gait analysis" to judge employee performance. These tools are often biased against neurodivergent staff who may work in non-traditional patterns.

- Sell or Trade Staff Biometrics: Employee fingerprints, facial scans, or health data (such as heart rate or "stress scores" from wearable devices) are strictly for security/access and shall never be shared, traded, or sold to insurance companies or data brokers.

- Use "Shadow" Monitoring: We prohibit the remote activation of webcams or microphones and the use of "always-on" location tracking on personal devices.

- Use Algorithmic Discipline: No staff member shall be disciplined or terminated based solely on a "risk score" or a "productivity benchmark" created by an AI. Humans, not algorithms, must lead our workforce.

- Require "Neuro-Surveillance": We explicitly ban the use of any technology meant to monitor "brain states" or "cognitive focus," as these are invasive and discriminatory.

Adopted by _____ this _____.