JAMES H. BINGER CENTER
FOR NEW AMERICANS
UNIVERSITY OF MINNESOTA

November 18, 2025

Co-Chair Sandra Feist & Co-Chair Peggy Scott
Legislative Commission on Data Practices
Minnesota State Legislature

RE: Written Testimony to the Legislative Commission on Data Practices
Healthcare Data Privacy Protections

Dear Co-Chair Feist, Co-Chair Scott and Members of the Legislative Commission on Data Practices:

My name is Ana Pottratz Acosta and I am a Visiting Professor at the University of Minnesota Law School, teaching Immigration Law and the Immigration and Human Rights Clinic, part of the James H. Binger Center for New Americans. I also hold permanent appointment as Professor of Law at Mitchell Hamline School of Law (MHSL) in St. Paul, MN, specializing in the areas of legal ethics, health law, immigration law and social determinants of health. My teaching responsibilities at MHSL include teaching the MHSL Health Law Clinic, which uses a Medical Legal Partnership (MLP) model, and overseeing the MLP program between Mitchell Hamline and Riverland Community Health, a Federally Qualified Health Center in St. Paul, MN. Under the MLP model used by the MHSL Health Law Clinic, law students working under my supervision provide legal services to patients of Riverland Community Health, our medical partner, as part of an interdisciplinary care team to address social determinants of health and improve health outcomes.

I present this written testimony to the Legislative Commission on Data Practices in my professional capacity as a law professor with specialized knowledge in health law, legal ethics and data privacy in healthcare settings. Specifically, I am presenting this testimony to offer this committee additional information on the existing data privacy protections under existing federal law, through the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), and Minnesota state law through the Minnesota Health Records Act (MHRA) and Minnesota Consumer Data Privacy Act. Additionally, given the highly sensitive nature of private patient data, I encourage this committee to retain or enhance existing data privacy protections under Minnesota state law to protect private healthcare data.

To provide relevant background on HIPAA, the statute had three main purposes: 1) to grant patients the right to access their own medical records, 2) to protect the privacy of a patient's

healthcare records, or protected health information (PHI), including limitations on the release PHI without of the patient's consent and 3) to create data security measures for storage and transmission of medical records containing PHI. Under HIPAA, PHI is defined very broadly and includes any individually identifiable information contained in an individual's health record and under the law, all *covered entities* and their business associates are required to comply with the healthcare data privacy protections contained in the law. Pursuant to HIPAA, covered entities include public and private health insurance plans, healthcare providers and healthcare clearing houses and business associates of covered entities include organizations that perform certain functions or activities, such as claims processing, billing or data analysis, on behalf of a covered entity.

In addition to HIPAA, the HITECH Act contains additional healthcare data privacy protections, including imposing additional requirements on business associates of HIPAA covered entities to ensure PHI is not disclosed unless authorized by HIPAA. The HITECH Act also created financial penalties for both covered entities and business associates for any breaches of unsecured PHI or unauthorized disclosures of PHI. These civil fines were established under HITECH to ensure both covered entities and their business associates took adequate security measures as healthcare providers transitioned to use of electronic medical records.

With respect to state law healthcare data privacy protections, the state of Minnesota, through the MHRA, has enacted more robust data privacy protections than exist under HIPAA by imposing more strict patient informed consent requirements prior to the release of PHI. More recently, through the Minnesota Consumer Protection Act, the state of Minnesota created additional data privacy protection measures under state law limiting the collection and sale of personal data.

While these additional patient consent requirements under MHRA and data privacy protections under the Minnesota Consumer Protection Act offer more protection than other states, there are still vulnerabilities in the area of data privacy, particularly over personal healthcare data. For example, Minnesota could enhance the existing protections under the Minnesota Consumer Protection Act to prohibit the sale of any personal healthcare data, even if anonymized, by HIPAA covered entities and business associates to data brokers. Accordingly, I urge the Legislative Commission on Data Practices to undertake a thorough review of existing healthcare data privacy protections under Minnesota state law and enact more robust protections over sensitive healthcare data.

Respectfully Submitted,

Ana Pottratz Acosta
Visiting Professor
James H. Binger Center for New Americans
University of Minnesota Law School