HIPAA, PHIPA AND PIPEDA COMPLIANCE STATEMENTS

Below are the steps Credproof Inc. (“Credproof”) takes to ensure your privacy and protection

Credproof is committed to and has implemented many safeguards to ensure its devices, services, websites and data systems (collectively “Products”) are compliant with the regulations and conditions set forth in the Health Insurance Portability and Availability Act (HIPAA), the Personal Health Information Protection Act (PHIPA), the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable personal health information legislation where it operates. Credproof is committed to the continuous improvement of its policies to ensure our Products incorporate state-of-the-art information technology privacy and security measures.

Credproof deploys its solution in data centers in **Canada, United States of America, United Kingdom, Ireland**, and new data centers are constantly added to meet the personal health information regulations in each region. Data in one region never travels into another, and all geographic boundaries are maintained to all scoped data. All solutions are deployed with redundancies and regular backups, in accordance with Credproof’s **Written Information Security Program,** available on request.

Credproof protects personal health information through the following integrated administrative, physical and technological safeguards:

DETAILS:

Administrative Safeguards. Credproof has implemented policies to ensure appropriate assignment of data access permissions and proper movement and handling of that data. Privacy training is an annual mandated event for all staff, as well as annual review of policy effectiveness during internal or third party auditing of our Products.

Physical Safeguards. The primary physical safeguard for Credproof is to not retain sensitive data in any public or private Credproof location other than those assigned for database management and quality assurance activities. Specific workstation usage, disposal, reuse and security measures are in place. Access to Credproof facilities are all

independently controlled via key access preventing walk-up intrusion. Credproof data centre uses a cloud-based architecture with inherent security measures including 24 hours monitoring, advanced fire protection systems, uninterruptible power and database redundancy. Annual audit of the facility security plan, disaster recovery plan, and contingency plans are in place.

Technical Safeguards. To further protect sensitive data, Credproof enforces unique software architecture that includes user identifications, various database audit logging, data integrity systems and verified backups, entity authentication programs, digital certificates, various levels of encryption (for data in rest, and in transit) and other custom architecture to further obscure sensitive data from threats.

OTHER INFORMATION:

Credproof will never share, sell, or trade Personal Identifiable Information (PII) or Personal Health Information (PHI) to third parties. Credproof does not use or disclose Personal Health Information, except as necessary in the course of providing its product and service to its clients. If disclosure of Personal Health Information is necessary at any point, it is used or disclosed strictly in accordance with the Personal Health Information Protection Act.

CONTACT

If you have further questions regarding our Privacy Statements, please contact our Chief Privacy Officer at privacy@immunodex.com or 1-437-889-2188