Outcome HIPAA Overview and Security Policy - US

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) was enacted to protect the privacy, security and distribution of individually identifiable health information. Healthcare organizations, which include health plans and health care providers, must comply with HIPAA or face significant sanctions from the U.S. Department of Health and Human Services, the government agency authorized to enforce HIPAA. Compliance with HIPAA is of wide-ranging importance because HIPAA specifies legal, regulatory, process, security, and technology requirements imposed on healthcare organizations that handle individually identifiable health information.

While Outcome Sciences, Inc. (“Outcome”) is not a healthcare organization, when Outcome facilitates the conduct of post-market approval research studies at various research sites who themselves are healthcare organizations, Outcome often handles individually identifiable health information. Therefore, although Outcome is not regulated by HIPAA, Outcome is nevertheless committed to handling individually identifiable health information in a manner consistent with U.S. federal laws and regulations relating to the security and electronic handling of protected health information, including but not limited to, applicable HIPAA requirements relating to security and electronic transfer, and any other federal mandates.

All of Outcome ’s post- marketing research solutions are fully consistent with HIPAA and mesh seamlessly with healthcare organizations’ existing HIPAA protocols. Outcome has extensive experience in customizing products for healthcare organizations and pharmaceutical companies, and has worked closely with them to facilitate healthcare organizations’ HIPAA compliance. Outcome has developed and managed the largest number of web-based ***e***Studies and ***e***Registries in the industry, and our on- line systems are used in over 2,000 hospitals in the U.S., including every major academic center.

Outcome has implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information. Outcome manages security through both physical and logical methods. Our systems and databases are maintained in a secure, access-controlled and monitored facility. The mechanisms we employ include encryption, authentication, intrusion detection, user-identification, secure storage and back-up, data redacting, and non-modifiable audit trails. In addition, external assessments of system security are routinely performed by an independent, expert third party.

In summary, Outcome’s systems are maintained according to high standards of health care information collection, handling and transmission. We regularly monitor technological, procedural and statutory changes which affect the protection of protected health information. This security policy is a dynamic document which will reflect our continuing vigilance to properly handle and secure information that we are trusted to maintain.