Data Privacy and Security Policy

The privacy and security of personal data and health information are of primary concern to Outcome Sciences, Inc. d/b/a Outcome ("Outcome"). Outcome carefully protects the confidential personal and health information provided to it by business partners and volunteer research subjects, healthcare professionals and health care institutions that maintain data. Outcome is committed to following applicable laws, rules and regulations in our use, collection and disclosure of such information. This Data Privacy and Security Policy is a dynamic document, which will reflect our continuing vigilance to properly handle and secure information that we are trusted to maintain.

I. For users located in the United States, the terms of this Section I shall apply:

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the rules and regulations implemented under HIPAA were enacted to protect the privacy, security and distribution of individually identifiable health information. Healthcare organizations, which include health plans and health care professionals, 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 is not a healthcare organization, certain of HIPAA's duties and obligations apply to Outcome when we serve as a Business Associate (as defined under HIPAA) of healthcare organizations, such as when Outcome facilitates the conduct of post-market approval research studies and quality improvement programs at various healthcare sites, which involves the use and disclosure of individually identifiable health information. Outcome is 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 legal mandates.

All of Outcome's post-marketing research solutions are consistent with HIPAA and mesh 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 eStudies and eRegistries 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.

II. For users located in the European Union, the terms of this Section II shall apply:

Under EU legislation, any information relating to an identified or identifiable natural person is "personal data." Personal data must be held in accordance with the legal framework set out in the Data Protection Directive 95/46/EC (the "Data Protection Directive"). With consent or pursuant to approvals from appropriate ethics committees, all personal data is stored on a secure database. All Outcome staff handling personal data receives training in the requirements of applicable laws and regulations. Outcome is committed to ensuring that personal health information (as sensitive data) is kept strictly confidential, however, personal data may be disclosed to regulatory authorities for the purposes of obtaining regulatory approval, or to comply with applicable legal requirements. Personal data may also be disclosed to certain third parties consistent with the terms of an informed consent obtained from data subjects whose personal data may be used for research activities, or as otherwise permitted by approvals from applicable ethics committees. Personal data may, at times, also be key-coded, and if then used, the method of key-coding is handled in a manner consistent with EU data protection principles. Individuals are entitled to access and correct personal data held about them if they so wish.

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions to enable U.S. companies to satisfy the requirement under European Union law that adequate protection is given to personal information transferred from the EU to the United States (the "Safe Harbor Principles"). The European Economic Area ("EEA") has also recognized the Safe Harbor Principles as providing adequate protection to personal data. The EEA includes the twenty-five members of the European Union plus Iceland, Liechtenstein and Norway. Outcome is committed to protecting personal privacy and adheres to the Safe Harbor Principles relating to the giving of notice, choice, onward transfer of information, access to personal information, security, data integrity and enforcement.

Where Outcome collects personal data directly from individuals in the EEA, it will inform them about the purposes for which it collects and uses personal data about them, namely the conduct of research that may involve their personal data. Outcome will only provide information to third party agents for the purposes of providing Outcome's services in a manner consistent with the principles named above. Outcome may transfer personal data to its United States office, to agents who are subject to the United States federal law regarding the protection of health information (the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")), as well as to agents who are not subject to HIPAA. However, in the event of transfers to Outcome's offices in the United States or to agents who are not subject to HIPAA, appropriate assurances are in place in the case of Outcome, and are sought from Outcome's agents. These assurances may include: a contract obligating the agent to provide at least the same level of protection as is required by the relevant Safe Harbor Principles, being subject to EU Directive 95/46/EC Safe Harbor certification by the agent, or being subject to another European Commission adequacy finding (e.g., the Swiss-US Safe Harbor Certification).

Outcome recognizes the importance of maintaining the privacy of information collected and/or stored online and has systems in place that protect data collected and/or stored online or via an electronic database. Outcome has implemented administrative, physical and technical safeguards to protect electronic personal data from loss, misuse and unauthorized access. In particular, Outcome is pursuing certification to the international security standards BS ISO/IEC 27001:2005 for information management systems. These standards implement the Organization for Economic Cooperation and Development's guidelines on privacy, security of information and network systems.

In order to maintain our information collection and transmission system to optimum standards, Outcome monitors amendments to technological, regulatory and legislative standards relating to the privacy and security of personal data.

III. For users located outside of the United States and outside of the European Union, the terms of this Section III shall apply:

It is Outcome's intention to ensure that all personal data provided to it, from anywhere in the world, is held appropriately and in accordance with the international data protection rules which apply to such personal data. Outcome intends that its standard practices and procedures with regard to the collection, use and disclosure of personal data will comply with local data protection laws, where applicable. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the "OECD Guidelines") set out general Privacy Principles. These OECD Guidelines form the core of most data protection laws globally. In order to ensure a high standard of protection for personal information held and processed by Outcome, personal data will be collected, used and disclosed by Outcome in accordance with the standards set out in the OECD Guidelines.

With the consent of the data subject or pursuant to other appropriate approvals, all personal data is stored on a secure database. All Outcome staff handling personal data receive training in the requirements of data protection related laws and regulations. Outcome is committed to ensuring that personal data is kept strictly confidential, however, personal data may be disclosed to regulatory authorities for the purposes of obtaining regulatory approval in accordance with applicable legal requirements, or otherwise to comply with applicable legal requirements. Personal data may also be disclosed to certain third parties consistent with the terms of unambiguous informed consent obtained from data subjects whose personal data may be used for research activities, or as otherwise permitted by other appropriate approvals. Personal data may, at times, also be key-coded, and if then used, the method of key-coding is handled in a manner consistent with OECD Guidelines. Individuals are entitled to access and correct personal data held about them if they so wish.

Where Outcome collects personal data directly from individuals throughout the world, we will inform them about the purposes for which we collect and use personal data about them, namely the conduct of research that may involve their personal data and any other relevant purposes. Outcome will only provide information to third party agents for the purposes of providing Outcome's services in a manner consistent with the principles described above. Outcome may transfer personal data to its United States offices, and those offices will hold such data in accordance with this policy. Outcome may also transfer personal information to agents, from whom appropriate assurances will be sought that the personal information will be handled in accordance with OECD guidelines and applicable local laws.

Outcome recognizes the importance of maintaining the privacy of information collected and/or stored online and has systems in place that protect personal data collected and/or stored online or via an electronic database. Outcome has implemented administrative, physical and technical safeguards to protect electronic personal data from loss, misuse and unauthorized access. In particular, Outcome is pursuing certification to the international security standards BS ISO/IEC 27001:2005 for information management systems. These standards implement the OECD's guidelines on privacy, security of information and network systems.

In order to maintain our information collection and transmission system to optimum standards, Outcome monitors developments in respect of technological, regulatory and legislative standards relating to the privacy and security of personal data.