IPMPC
International Pharmaceutical & Medical Device Privacy Consortium

April 8, 2019

IPMPC Principles for U.S. Privacy Legislation

Over the last century, medical science has transformed human health and dramatically increased life expectancy. The life-saving treatments available today were made possible by an environment that fostered medical research. The scientific process used in medical research relies on the ability to effectively collect, analyze and re-analyze patient health information. Researchers at pharmaceutical, biotech, diagnostic, and medical device companies need access to patient health information in order to develop new drugs and medical technologies to improve and save lives.

Effective health care delivery also relies on the ability to use and share patient health information. Health care today is increasingly information driven. Doctors often need detailed information about a patient in order to determine which drug or medical device will be optimal for that individual. Those involved in the delivery of healthcare—not just physicians, but increasingly health insurers, and quality assurance organizations—have similar, legitimate data needs including for evidence of health outcomes. Throughout the health care system there is a common need for ready access to health data.

Pharmaceutical and medical device companies share this need for health data – to conduct research, to identify beneficial or harmful side-effects of drugs or medical devices, to determine the effectiveness of new treatment protocols, to seek out genetic patterns in the effectiveness of drug therapies or medical devices, and to locate appropriate individuals to be invited to participate in research studies based on increasingly specific and difficult to satisfy criteria. As legislators in the U.S. consider new information privacy protections, it is also important to keep in mind the legitimate needs of the life sciences community to access and use health data.

Members of the International Pharmaceutical & Medical Device Privacy Consortium (IPMPC) share a commitment to responsible data stewardship and protecting patient privacy. As policy makers at the state and federal levels consider the adoption of comprehensive data privacy legislation, we urge consideration of the needs of the pharmaceutical and medical device sectors. We recognize that a legal framework is needed that provides individuals with meaningful information privacy rights. That framework must not only provide strong and effective protection for personal information but also facilitate scientific discovery and medical innovation. Therefore, the International Pharmaceutical & Medical Device Privacy Consortium **SUPPORTS** comprehensive U.S. privacy legislation that:

1. **Recognizes an appropriate distinction between identifiable information ("personal information") and information that has had identifiers removed ("anonymized information").** *The right to informational privacy must always be balanced against competing societal interests, such as the need for access to data to support scientific innovation. Data privacy laws should be focused on promoting transparency around the collection and use of personal information and on protecting individuals from injury – whether tangible (e.g., financial harm) or intangible (e.g., damage to reputation, embarrassment). As the identifiability of information decreases, so does the potential for the collection, use, or disclosure of that information to cause real injury, and so do the legitimate interests of individuals in controlling such information.*

2. **Recognizes an appropriate distinction between identifiable information ("personal information") and information that has had identifiers masked ("pseudonymized information").** *Pseudonymization is a privacy-enhancing safeguard that involves replacing directly identifiable information (e.g., name, contact information) with a securely-held code before this information is disclosed to third-parties. Data privacy laws should recognize that as to the recipients of pseudonymized data (i.e., those who do not have access to the re-identification key), the information is effectively anonymized. For example, recipients of pseudonymized data have no reasonable ability to respond to data subject requests for access or erasure.*

3. **Appropriately balances the rights of individuals to control the collection, use, and dissemination of personal information about them with researchers' need to be able to collect, use, and share information for scientific advancement.** *Medical discoveries rely on the ability to safely and effectively collect and analyze personal information concerning patient treatment and outcomes. Without personal information, scientists would lack insight into the causes of certain conditions and diseases, and development of curative and preventative measures would be impossible. The ability to sustain and expand on such scientific innovations depends upon the continued availability of patient information to meet researchers' needs.*

4. **Promotes the implementation of privacy safeguards in a manner that is proportional to the risks presented on a case-by-case basis.** *In considering the safeguards that are appropriate in the context of a particular data processing activity, the nature, scope, context, and purposes of the data processing may be relevant, as are factors such as the identifiability and sensitivity of the information. Organizations should be encouraged to assess the level of risks on a case-by-case basis and implement corresponding protections that are fit-for-purpose. For example, whole genome sequencing presents different privacy risks as compared to genetic testing for a particular DNA sequence. In turn, forensic DNA testing presents different risks than, e.g., diagnostic DNA testing. Similarly, use of a retinal scan for biometric identification purposes presents different risks than the use of retinal images to diagnose health conditions. Privacy laws must, therefore, allow for flexibility in determining the safeguards appropriate to a particular use case.*

5. **Appropriately takes into account the protections that already apply to personal health information under various frameworks and the deliberative rulemaking process that went into crafting federal health privacy rules that balance individual rights with the needs of the health care community.** *The use and disclosure of health information is regulated under, inter alia, the Health Insurance Portability and Accountability Act (HIPAA); the Federal Policy for the Protection of Human Subjects (or "Common Rule") and FDA human subject protection regulations; and Good Clinical Practices guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. These regulations and standards were carefully crafted over a period of years and include detailed requirements. As new laws are developed to address gaps in existing requirements and provide more comprehensive privacy protections, efforts should be made to harmonize new and existing frameworks.*

6. **Appropriately distinguishes the rights that are afforded to individuals acting in a personal capacity as consumers of goods and services from individuals acting as employees or in a professional capacity.** *Employers have a legitimate need to evaluate employees' performance and to manage their activities. Similarly, businesses (and government) have a compelling interest in being able to measure the performance of professionals in a variety of sectors. In the health care sector, for example, performance metrics are important to ensuring quality of care and cost effectiveness.*

7. **Provides individuals with appropriate recourse in case their rights are violated by empowering enforcement authorities at the federal and state levels, while at the same time taking into account organizations' good faith efforts to comply.** *Individuals should be able to make complaints to appropriate regulatory bodies in the event their privacy rights are violated. Enforcement authorities should be given the resources necessary to exercise appropriate oversight and take required corrective actions.*

8. **Leads to harmonization of privacy requirements in the United States rather than a confusing patchwork of different requirements.** *Differing privacy standards across the US raise the cost of compliance. In many cases, it is impractical for businesses to modify their US business practices to account for state and local variations.*