IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

April 2019

The Role of Personal Data in Healthcare

Introduction

Over the last century, medical science has transformed human health. At the start of the 20th Century, the average life expectancy in developed countries was slightly over 45 years. Today, life expectancy exceeds 75 years. The 20th Century witnessed the eradication of smallpox and considerable progress toward the eradication of polio and other infectious diseases that until such time killed by the millions. Immunizations and antibiotics greatly reduced diseases such as tuberculosis, whooping cough, diphtheria, and typhoid fever. In this golden era of medicines research, the structure and function of DNA was elucidated, leading to the mapping of the human genome. Numerous medicines from immunosuppresives to antidepressants to contraceptives were developed, improving and saving lives. Prosthetic limbs have been invented that closely mimic natural body motions for amputees; advances in medical imaging have enabled doctors to quickly and accurately identify injuries and diseases; and artificial organs have been engineered that can replace natural organs, allowing patients to return to a normal life.

The life-saving treatments available today were made possible by an environment that fostered health research and recognized that medical innovation benefits society. Medical discoveries rely on the ability to safely and effectively collect and analyze personal data concerning patient treatment and outcomes. Without personal data, scientists would lack insight into the causes of certain conditions and diseases, and development of curative and preventative measures would be impossible. In each of the steps in the scientific process – i.e., an observation leading to a hypothesis, followed by testing and then confirmation – the ability to effectively collect, analyze, and re-analyze patient information is crucial. The ability to sustain and expand on such scientific innovations depends upon the continued availability of patient information to meet researchers' needs.

Personal data is not only critical to the work of the biopharmaceutical and medical device industries; the ability to use personal data has healthcare ramifications for policy makers and government as well. Analysis of personal data is an important public health tool used to quickly identify and remedy adverse events in certain populations when they are first reported. Personal data also shapes healthcare policies which are based on information about the costs and benefits of interventions. In short, personal data has a profound and often understated impact on many aspects of healthcare.

The Importance of Personal Data to Healthcare

As described above, the ability to use personal data is critical to medical innovation, public health, and healthcare efficiency. These uses are further summarized below:

- The development of new medical interventions demands extensive testing to ensure patient safety and effectiveness. Moreover, the U.S. Food and Drug Administration and other health authorities are increasingly requiring the evaluation of the effectiveness of medicines and medical devices in real-life settings creating a need to collect 'real-world evidence' derived from patient medical records.

- Advances in life sciences are enabling far more targeted delivery of medicines to patients. Such "personalized" medicine looks at the genetic and phenotypic characteristics of individual patients to determine which treatments will be most safe and effective.

- Financial pressures demand that healthcare resources are used efficiently. Data about healthcare resource use and health outcomes can help inform policy development to increase healthcare efficiency.

- With the adoption of electronic health records (EHRs) and platforms for sharing EHRs, new opportunities are arising for the study of patterns of disease development and progression, providing new insights into the causes and control of disease.

Research uses of personal data can be further broken down into the following categories:

- **Discovery and early-stage development** is the first stage in medical product R&D. In the development of new drugs, for example, this often involves the testing of human biological samples to validate or disprove a research hypothesis.

- **Clinical research** involves the evaluation of the safety and efficacy of medical interventions under controlled conditions in human subjects. Clinical research is highly regulated. Clinical research in the United States is subject to regulation including requirements of U.S. Department of Health and Human Services agencies such as the Office for Human Research Protections, the U.S. Food and Drug Administration, and the National Institutes of Health, as well as international standards, such as the good clinical practice guidelines issued by the International Council for Harmonization.

- **Pharmacoepidemiology and Medical Device Epidemiology** is the study of the use and effects of drug therapies and medical devices in large numbers of people. As an example, in the field of cancer, pharmacoepidemiology examines the effects of medications on cancer risk, disease prevention, and response to treatments, as well as any adverse and/or long-term effects of chemotherapeutic and other pharmacologic agents used to treat cancer.

- **Pharmacogenomics** focuses on understanding how variability in genes impacts drug response. Thus, pharmacogenomics seeks to correlate individual differences in adverse effects and treatment effectiveness with gene expression for drug-metabolizing enzymes, drug transporters, drug receptors, and proteins involved in pathway signaling.

- **Pharmacoeconomics and medical device health economics** evaluate the costs and benefits of a pharmaceutical or medical device product. Pharmacoeconomic and medical device health economic studies serve to guide optimal healthcare resource allocation.

- **Pharmacovigilance and medical device vigilance** encompass the science and activities relating to the detection, assessment, understanding, and prevention of adverse events or any other drug/device related adverse effects. Pharmaceutical and medical device companies have ethical and legal obligations to accurately collect, analyze, and report adverse events in a timely fashion both during clinical trials and after a drug is on the market. In the U.S., pharmacovigilance and medical device vigilance are specifically regulated by the U.S. FDA.

Safeguards Around Personal Data

A number of safeguards already operate within the healthcare delivery and research communities to ensure the protection of personal data:

- When identifiable personal data from a research patient is collected directly from an individual by a healthcare provider or clinical research organization, the patient is informed of the scope of the data to be collected, the purposes for which it will be used, the length of use or storage, and the identity of permitted recipients. The patient is asked to provide informed consent to participate in the research and an authorization to permit use and disclosure of identifiable health information.[1]

[1] The scope of an individual authorization to use and disclose identifiable health information may vary. It can be limited to one individual clinical study or it may cover future medical

(Continued)

- Professional standards govern the use and disclosure of personal data. Clinical researchers are subject to Good Clinical Practice (GCP) standards which require investigators to safeguard research subject data, obtain written authorization to access a subject's medical records, and protect the confidentiality of the subject's identity when the results of the trial are published.

- Institutional Review Boards review clinical research protocols (a document that describes the objective(s), design, methodology, statistical considerations, and organization of a study) and assess the risks to individual data subjects.

- In clinical research studies, patient direct identifiers are highly protected and often removed. The data is key-coded before being sent to the pharmaceutical or medical device company sponsoring the study. The specific re-identification key is held by the clinical investigator.

U.S. Privacy Legislation

To protect both the right to privacy and the objectives of advancing medicine in privacy legislation at the U.S. state and federal levels, policy makers should:

- Recognize key-coding as a measure for ensuring that privacy is embedded into the design of clinical research studies. Correspondingly, requirements related to the retention, use and disclosure of key-coded data for research purposes should be distinguished from requirements applicable to "personal data." Further, the exercise of the rights of access and rectification of personal data should be directed towards the holder of the key rather than the holder of the key-coded data.

- Continue to allow clinical research subjects to provide broad authorization to the use and disclosure of their personal data for secondary biomedical research purposes, such as understanding disease mechanisms and further research. Researchers frequently encounter difficulty predicting outcomes associated with medical testing and treatment.

(Continued)

research on the condition or disease in question. Healthcare companies seek to provide patients with the information they require to make informed decisions regarding the use of their identifiable medical information.

Further use and disclosure of patient data is often necessary and should be able to be performed with the broadly granted authorization of the patient.

- Recognize the limitations on the ability of researchers and healthcare professionals to obtain authorization without disproportionate efforts when identifiable health information is collected other than directly from data subjects. For example, a requirement to obtain individual authorization before conducting records-based research would greatly increase the costs of such studies and may lead to skewed datasets. Similarly, when drug or device adverse events are reported by persons other than the patient, obtaining consent can be costly and may conflict with legal requirements concerning adverse event reporting.

- Limit the application of a "right to deletion" when it interferes with an ongoing study. For example, once a person agrees to participate in a clinical study, the scientific integrity of the study analysis depends upon the ability of the clinical investigator to accurately track and correlate data about that person, up until the point at which the person either completes participation in the study or withdraws from it, whichever is sooner.[2] Upon withdrawal, no further data about the person is collected; however, it is essential that the data about that person that already has been collected may be retained and analyzed. Otherwise the validity of the study may be compromised.

- Require breach notification only where the loss of or unauthorized access to personal data poses an actual risk of harm to data subjects. Requiring notification in other circumstances will divert resources from other privacy and security safeguards. In particular, breach notification requirements should not apply to key-coded data, unless the key has also been accessed by unauthorized persons.

- Not require separate rules for genetic information or specify that genetic data is in and of itself identifiable. All medical data, including genetic data, must satisfy equally high standards of quality and confidentiality. Genetic information is part of the entirety of every individual's health information and does not represent a separate category. Moreover, genetic data is identifiable only to the extent that a reference dataset that

[2] S*ee* HHS Guidance on Withdrawal of Subjects from Research (2010)*, available at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/guidance-on-withdrawal-of-subject/index.html;* FDA Guidance on Data Retention when Subjects Withdraw from FDA-Regulated Clinical Trials (2008)*, available at https://www.fda.gov/downloads/regulatoryinformation/guidances/ucm126489.pdf.*

links the data to an identified person is accessible. Thus, genetic exceptionalism is inappropriate.

Conclusion

As data privacy legislation is considered at both the U.S. state and federal levels, special consideration should be given to the impacts on all stakeholders in the healthcare ecosystem. The right to privacy and the activities associated with advancing medicine and demonstrating real-world effectiveness must *both* be protected in any legislation that is implemented.