

Elizabeth Litten, JD  
[ELitten@foxrothschild.com](mailto:ELitten@foxrothschild.com)

## **Health Information Property Act**

Good morning and thank you for giving me the opportunity to explain the purpose behind and need for the Health Information Property Act. My name is Elizabeth Litten, and I am a partner with the law firm of Fox Rothschild LLP, where I serve as co-chair of the Privacy and Data Security Practice Group and as the firm's HIPAA Privacy & Security Officer. I have practiced health law my entire career, representing hospitals, physicians, health plans, and other entities in the health care industry. I serve as a member of the Governing Board of the New Jersey Integrated Population Health Data Project, a project created by the NJ Legislature in 2016 with the goal of enabling the integration of data held by State agencies and publicly supported programs for public health research purposes. I serve as the Governor's appointee of a member of the public with legal expertise and an interest in protecting the privacy and security of individually identifiable health information.

The Health Information Property Act creates a way for consumers to claim the right to control their health-related data. This is data that, as I speak, is being used and sold in a multi-trillion dollar marketplace without consumers' knowledge or consent. This is data that is being used in a manner not expressly described in the HIPAA notice consumers are given by their providers and health plans (the Notice of Privacy Practices), and likely without the providers' or health plans' knowledge or agreement. I have reviewed hundreds of business associate agreements or "BAAs" (the HIPAA-required agreements between health care providers or health plans and their service providers that detail the parties' obligations under HIPAA), and have never seen a BAA that permits the de-identification of protected health information expressly for the purpose of its commercial sale. Nonetheless, this is happening.

According to William W. Stead, M.D., Chair, National Committee on Vital and Health Statistics in a 2017 letter to Honorable Thomas E. Price, M.D. Secretary, Department of Health and Human Services: "Even data properly de-identified under the Privacy Rule may carry with it some private information, and, therefore, poses some risk of re-identification, a risk that grows into the future as new datasets are released and as datasets are combined."

Further, "Consumers are rarely aware of when their data are being de-identified for a new purpose. Unlike disclosures of PHI, where the Privacy Rule requires that individuals have the right to an accounting of disclosures of their PHI to third parties with certain exceptions, the subjects of de-identified datasets may not know how often their data are disclosed in de-identified form as de-identified data are not subject to the HIPAA Privacy Rule. Even disclosure of a "limited data set," a data set with most, but not all, of the Safe Harbor identifiers removed, is not subject to the requirement for a covered entity to maintain an "accounting of disclosures," permitting an individual, on request, to obtain a list of recipients of their protected health information.

Moreover, it's increasingly common for consumers' medical record data to be combined with non-health-related data, increasing the risk of re-identification. Data analysts are now able to augment health data with geographic, socio-economic, and other public and private information to gain new scientific insight or advance a commercial goal."

An article published in last month's "Nature Medicine" magazine entitled "Privacy in the age of medical big data" examines the legal and ethical considerations big data brings to patient privacy. The authors highlight a difference between US and EU health data protection regimes -- the US protections are custodian-specific, whereas the EU provides blanket protections that do not vary based on who creates or holds the data. The authors conclude: "The future of big data privacy will be sensitive to data source, data custodian, and type of data, as well as the importance of data triangulation from multiple sources." The Health Information Property Act takes into consideration each of these factors, seeking to strike the right balance between enhancing individuals' ability to claim their right to keep a sensitive category of personal data (individually identifiable health information) private, while not interfering with the use of big data for legitimate research and health improvement purposes.

Most importantly, this Act only affects entities engaged in the *commercial sale* of health information or data derived from health information (i.e., de-identified health information). It has no impact on the use or disclosure of health information permitted under HIPAA, such as use or disclosure for payment, treatment, health care operations of a Covered Entity, involvement in a patient's care, research, or public health purposes. It also has no impact on disclosures of de-identified data when the disclosures do not involve remuneration to the entity disclosing the data.

Thus, the Act should not impact the way in which health plans, hospitals and other providers use and disclose data, nor should it impede research or the uses or disclosures of government entities or their contractors of health information.

Oregon consumers will become empowered under the Act because third parties will need to get their express permission, in the form of a HIPAA Authorization, before they can engage in the *commercial sale* of the consumer's health-related information. The consumer will have the opportunity to agree to the sale, to decline the sale, to put conditions on the sale, or to prohibit the sale.

The results will be twofold: (1) consumers will be able to stake a right to control and claim the value associated with their health information (a value currently taken unilaterally from the consumer); and (2) the purchasers of large sets of aggregated data will, over time, be able to see what percentage of that data has been consumer-authorized. We view this as an important first step toward data use transparency and accountability.