Advancements in the storage and management of electronic health data have created increased opportunities for exploring the secondary uses of these data (e.g., for quality, biomedical research, and public health studies). While enabling research, privacy violation has become a major concern when these data are released or shared. Considerable efforts have been made to protect patient privacy through regulations and laws, such as the Health Insurance Portability and Accountability Act (HIPAA), which aim to protect the confidentiality, integrity, and availability of electronic health information. Accordingly, numerous studies have been focused on the development and evaluation of computational techniques for protecting the privacy of individuals while still making the data useful for research purposes. In this presentation, an overview of privacy protection approaches will first be provided followed by a description of key concepts related to k-anonymity, a popular anonymization approach. The presentation will conclude with a discussion about on-going experiments for exploring extensions to the k-anonymity algorithm that aim to address the heterogeneous needs of different researchers while preserving privacy and utility of datasets.