**SCANNER Legal Analysis**

Access to identifiable health information for research using either clinical or claims information is subject to regulation at both the federal and state level. Federal regulations established to implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA) set the conditions under which providers and plans can access, use and disclose identifiable information for research purposes. In addition, the Common Rule regulates research with identifiable patient data conducted at facilities receiving federal research dollars. Both HIPAA and the Common Rule generally require patient authorization for the use of identifiable data for research purposes, although this requirement can be waived in certain circumstances. Research using data that is not readily identifiable, however, is subject to fewer (if any) legal constraints. Consequently, researchers often seek to access data in de-identified or less identifiable form.

These rules apply to a data holder accessing information in its own records (such as a provider accessing information in his or her medical records system) and the disclosure of information to other parties.

In general, access to or disclosure of identifiable health information for research purposes requires the prior authorization of the persons who are the subjects of the information. (45 CFR 164.510) However, consent is not required in certain circumstances such as accessing health information in order to prepare for research, e.g., to formulate a hypothesis, or when the information is about a deceased person. (45 CFR 164.512(i)(1)(ii)) Even when the law requires an individual’s authorization, an Institutional Review Board (IRB) or Privacy Board may waive this requirement in certain circumstances, such as when the research involves no more than minimal risk or could not practicably be carried out without a waiver. (45 CFR 164.512(i)(1)(i), (i)(2)(ii)) When authorization is required, it must describe the research in sufficient detail. (45 CFR 164.508 (c)) Providers or plans accessing or disclosing identifiable information for research must use the minimum necessary amount of information needed to address the research question. (45 CFR 164.502(b))

Less identifiable data has fewer restrictions under HIPAA. For example, entities may access or disclose a LDS without obtaining prior authorization of the data subjects. (45 CFR 164.514(a)) An LDS must be stripped of 16 categories of identifiers – for example, name and street address – and the researcher must execute a data use agreement that sets forth the permitted uses and a commitment not to re-identify the information. (45 CFR 164.514(e)(4)) In addition, information that meets the HIPAA standard for de-identification – i.e., raises a very low risk of re-identification – may be used for any purpose. (45 CFR 164.514(a)) Entities often endeavor to access and disclose information for research purposes that is either de-identified or in LDS form to best protect the privacy of the data subjects and to ease regulatory requirements.

Research supported with federal funding from HHS and most of its sub-agencies is also subject to the Common Rule. (45 CFR 46.10 et seq.) Under the Common Rule, research using information gleaned from electronic medical records is subject to expedited review by an IRB (review by one member of the IRB, versus full IRB review). (45 CFR 46.110) If the researcher is receiving identifiable information, the researcher must obtain the consent of the data subjects. (45 CFR 46.116) The requirement to obtain consent may be waived by an IRB under similar circumstances as those applying under HIPAA: if (1) the research involves no more than minimal risk; (2) the waiver will not adversely affect the rights and welfare of the patients; (3) the research could not practicably be carried out without the waiver; and (4) when appropriate, the subjects are provided with additional pertinent information after participation. (45 CFR 46.116(d)

States also regulate the use of identifiable health information for research. The HIPAA Privacy Rule negates or takes precedence over conflicting or less protective state privacy laws (45 CFR 160.203) However, if a state law provides greater protections for patients – such as requiring specific authorization for a particular use of health information – that law remains in effect. Some of these state laws directly regulate uses of identifiable health information for research; others implement greater protections than HIPAA for certain types of sensitive data, whether accessed for treatment, research or other purposes. A state law is only applicable and binding on institutions located within that state.

States also are using funds from ARRA to create infrastructure to enable exchange of electronic health information among providers, patients, and relevant state health agencies. Such health information organizations (HIOs) often adopt policies that govern participating entities that establish greater restrictions on data collection, use and disclosure. Such restrictions are typically applicable only to the HIO and its members.