A Question of Data Security

A clinician has received an e-mail request for consultation asking him to provide information about a certain group of patients seen in his local clinic. The clinician is concerned about the new Health Insurance Portability and Accountability Act (HIPAA) regulations as they apply to confidentiality of patient information but also is overwhelmed by the volume of information and the technology required for data security. How should this clinician proceed?

Solutions

The issue with retrospective studies is what will happen to confidentiality as the results are reported. What are the requirements for obtaining permission to access identifiable information for research in this case? If the information is not identifiable, the Privacy Rule does not apply. However, the spirit of HIPAA needs to be maintained in how the data are reported, especially in how results of any individual patient or subject are reported. The investigator has the responsibility to ensure anonymity of the patients in the way a statistician creates the limited data set (LDS), in which the risk is small that the information could be used alone or in combination with other information to identify a person, but the information is not completely "deidentified" (for example, some dates, such as birth dates, are allowed). An LDS agreement must be obtained by this clinician from the covered entity, but such access does not have to be tracked. This option is available only for research, health-care operations, and public-health purposes. The institutional review board (IRB) will need documentation of the approved LDS agreement when the research project is submitted for IRB review and approval.

Charles H Halsted
University of California, Davis
School of Medicine
Davis, California

I needed some time to discuss the question with experts in this field, and I now have a short and possibly disappointing answer because our law does not differ very much in this respect from US law. We have two acts dealing with this problem: a general Privacy Act and the Medical Research Involving Human Subjects Act. Both always require patients' consent for their own doctors and for others to use data for any purpose. In this case, the clinician who was asked to provide particular patient data should have to ask written permission from the patients to do so, fully explaining who asked for it, for what research, and who will use the data. This will certainly be a time-consuming job, so he probably will refuse to do it. If the research is important and he is willing to provide the information asked for, he would be wise to contact his institutional review board, his hospital lawyer, or the regional or national medical-ethics committee. In general, a request like this one will be declined.

John Overbeke
Dutch Journal of Medicine
Amsterdam, the Netherlands

First, the clinician should understand that the Privacy Rule makes it the responsibility of the covered entity (CE) to safeguard protected health information (PHI). The clinician should contact the CE's privacy officer to see whether it is even allowable for the clinician to provide the requested information. If so, the clinician should determine whether the information request asks for a data set that contains individually identifiable health information, which is PHI. The Privacy Rule considers information to be identifiable if it includes the obvious identifiers (for example, name, medical record number, Social Security number, and telephone number) but also if it includes such identifiers as date of birth, service, diagnosis, and so on and any geographic subdivision smaller than a state. (See the Privacy Rule for a complete list at *www.hhs.gov/ccr/hipaa/*.) If the data set is stripped of all those identifiers, the Privacy Rule does not apply. If the data set contains any of those identifiers, the information is considered to be PHI, and the Privacy Rule applies.

If the data set contains identifiers that include only dates and geographic loca-

tions (excluding streets and postal addresses), the CE may consider sending it as an LDS. Whenever an LDS is used, the recipient and the CE must enter into a data-use agreement (DUA). An LDS is allowed to be shared only for research, public-health inquiries, or the CE's health-care operations. If the request is for research and contains identifiers, the clinician should submit a research application to his IRB; this process is fairly involved and requires that the clinician fully understand the collaborator's request and how the data set will be used and take responsibility for the research activities in which he has been asked to participate. If the request is for other purposes, the clinician should contact his CE's privacy officer for information on how, or whether, to proceed.

David Gary
Kaiser Foundation Research Institute
Oakland, California

New Question: A Question of Electronic Add-ons

A journal has started to include Web-only items that supplement the printed content. Most of those items are videos, but some are still images, articles, or other text. The staff of the journal and its parent organization lack the time and expertise to determine how best to deal with such material, for example, to work out technical difficulties when files are too big, formats are odd, or labeling is not adequately integrated (if it is there at all) while making sure that the Web supplements are rich in scientific content and easily navigated. The electronics department sometimes wants just to "reject" potential Web-only items, whereas the editorial staff wants to make them work. The editor of the journal seeks your guidance regarding this situation. What would you advise her?

The situations described as new questions in this column are not necessarily based on actual situations, and the ones that are may have been modified to focus the question. Send your responses to the new question to Della Mundy, Department of Medical Editing, Kaiser Foundation Research Institute, 1800 Harrison Street, 16th Floor, Oakland CA 94712-3429. Telephone (510) 625-2373; fax (510) 625-5231; e-mail *della.mundy@kp.org*.