AbstractID: 6021 Title: Panel: HIPAA Compliance and the Medical Physicist

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) made sweeping changes in the ways in which information regarding individuals' health care must be stored and transmitted electronically. Most AAPM members will have some familiarity with the resulting changes to policy and procedures implemented by health care providers and hospitals. The roll-out of Rules developed by the Department of Health and Human Services (HHS) in response to the Act is now approaching completion. With the dust beginning to settle it is a good time to review what is and is not required under the HIPAA umbrella.

The intent of the Act is laudable. It contains provisions to safeguard an individual's access to their own health care information and some degree of control over its use ("Privacy"), provisions mandating standardization of electronic information exchange for health information in order to streamline transmittal of information between health care entities ("Electronic Data Interchange"), and provisions requiring that covered entities take certain measures to safeguard individuals' information against unintended exposure ("Security").

Unfortunately, as is often the case with sweeping Federal regulation, there is a great deal of misinformation and confusion in the marketplace about the Rules and their implications. This arises partly because, while most of the requirements are clear, the detailed mechanisms for compliance must be developed and implemented locally. This is a situation quite analogous to radioactive materials licensing, with which we are all familiar. Often one is unsure of one's degree of compliance until one is actually inspected, a very uncomfortable place to be when there are both fines and bad publicity at stake. Uncertainty creates ample opportunity for unscrupulous consultants to prey on the anxiety of health care administrators by recommending excessive or misdirected "compliance" measures, thus compounding an already difficult transition. We have all seen this dynamic in action.

Another unfortunate outcome of the poorly-informed implementation of layers of unbending bureaucracy in the name of compliance is that sometimes restrictions are imposed locally on information flow which are ultimately against the best interest of the patient. For instance, an absolute local prohibition on releasing patient-specific treatment planning information may be directly in conflict with a Medical Physicist's need to send problematic data to a vendor to obtain timely resolution of a software anomaly.

The bulk of our attention in this session will be directed to clarifying the impact of the Rules on the practicing Medical Physicist. The question is not easily answered as the impact on a given Medical Physicist depends very much on the situation in which the Medical Physicist operates. We have in common that many of us act as *de facto* Information System managers in our departments and as such have a certain degree of practical responsibility for monitoring access to patient-specific information. The degree to which we are formally responsible for compliance may vary greatly, though, depending on the specifics of our contractual relationship to the hospital or other entity for which we are performing services. It is in the Medical Physicist's interest to be clear regarding both the responsibilities and the restrictions on practice that might be included in any agreements regarding HIPAA compliance that they might be asked to sign as a condition of employment. A good working knowledge of the basics of the Act and the Rules is a useful starting point.

We are fortunate indeed to have four expert Panelists representing four different perspectives on these questions. They are respectively (in order of their presentations) a member of the American College of Radiology's legal office, the Chief Privacy Officer for a major vendor of Radiation Oncology information management systems, the Local Security Coordinator for a mid-sized Regional Hospital, and a Senior Analyst with the Department of Health and Human Service's Office of Civil Rights (responsible for enforcement of the Rules).

The goals of this Panel are to

1. Briefly review the scope, structure and timeline of the Act and subsequently developed Rules, and introduce some of the specific jargon of HIPAA.

2. Clarify to whom the Rules apply and the chain of responsibility for compliance.

3. Discuss the specific impact on Medical Physicists of HIPAA and the local implementation of compliance programs.

4. Dispel some common myths about the requirements imposed by HIPAA and, conversely, highlight compliance issues that may be less widely appreciated.

5. Suggest some proactive strategies that Medical Physicists can employ to prevent conflicts with local compliance policy.