HIPAA Privacy and Security Factual Questions

Richard D. Marks
Davis Wright Tremaine LLP

Fact Issues (each of which also requires knowing the applicable legal standard):

1. What sort of access control is required? Can each access of protected health information (PHI) in a patient's record be logged, showing who called up the file? Can a doctor or nurse obtain access using a colleague's access authorization? What about doctors and medical students on rounds? What are the penalties for not implementing proper logging procedures? For not enforcing them vigorously? What kind of software can perform this kind of logging? Is it available today on the market?

2. What protections must be implemented for terminals where PHI will be accessed? Must nurses' stations be secure areas? If so, how secure? What about monitors in ICUs and similar facilities? Sign-in sheets in doctors' offices? What surveillance must be implemented for these areas?

3. What sort of system is required for generating and tracking "consents" and "authorizations," associating them with particular PHI, and allowing various uses (*e.g.*, care, research, marketing) of particular portions of the PHI? Are systems of this kind commercially available?

4. What kind of access procedures will satisfy HIPAA requirements and not impede patient care? Passwords alone? Passwords with SecureID or similar procedures? Biometrics?

5. What happens if a health care professional attempts to log on to get access to medical records in an emergency, and makes a mistake in their input of the password or other required information? How many attempts can be allowed before the system locks them out? What are the emergency access procedures? Must the doctor or nurse then be physically identified by a member of the security staff, in essence to revalidate that staff member? How will that be done? How long might it take, especially in an emergency setting? What if patient care suffers – what are the malpractice issues?

6. How can the logon, identification, and other required attributes of data protection, in transit and at rest, be satisfied without resort to asymmetric encryption techniques?

7. How can a medical professional or an administrator determine what to request under the "minimum necessary" disclosure standard? Where does one find the industry-standard guidelines to make these judgments? How do they change in the face of a medical emergency? What procedures are required (or prudent) for a hospital or a physician practice to review the scope of these requests after the fact? What if there is a question of excess PHI requested? Can the professionals involved in making the original request appeal? To whom? ? Must the requesting provider report the matter to HHS, and, if so, at what point? What guidelines will HHS use to review requests for disclosure? What malpractice jeopardy is there for making too narrow a request?

8. To what extent will the standard of care in the security industry require that protected health information (PHI) be stored in encrypted form? Are systems available on the market to perform this kind of storage?

9. Must voice communications systems be encrypted under HIPAA?