

Validating EMR Audit Automation

Carl A. Gunter

University of Illinois

Much effort in recent years has gone into the problem of how to audit accesses to Electronic Medical Records. This effort is motivated by the problem that there are high risks in denying access to hospital personnel, who often need access to the EMR as they handle patient emergencies, so there is a reluctance to prohibit access to most personnel. There is a hope that after-the-fact reviews can determine whether accesses were legitimate, hence providing access when essential but deterring and limiting illegitimate accesses. However, since the amount of data involved in a review may be too much for manual processing so automated techniques are important. There has been a lot of progress on such automated techniques, but the question is: how does one validate that a technique is effective. I'd like to discuss some of the alternatives that have been explored for this problem. The obvious gold standard is getting experts to help with a sample of illegitimate accesses. So far only a couple of papers in the research literature has had experts that could contribute in this way. The primary alternative technique might be called the Random Object Access Model (ROAM). The idea of ROAM is to add random events to the audit logs and look to see if the audit analytic engine flags them as meriting attention. I'll talk about variations on the implementation of this strategy and discuss some of the techniques that have been validated in this way. I would particularly like to speculate on moving beyond this approach with other types of validation. One of these, the Random Topic Access Model (RTAM) has shown some promise and will be offered for discussion.