INFORMATION SYSTEM AND SECURITY

MEDICAL DATABASE SECURITY

NAME:V RITHIK

REG.NO:19MIS1189

Prof: Rajesh Kumar

NEW\_IDEA FOR MEDICAL DATABASE SECURITY:

SECURITY ISSUE:

As many others have pointed out, the main problem with information security in health care is not technology, but a lack of cohesive security policy. Policy must shape technology, not vice versa. Security policy defines what is to be protected, to what rea­ sonable degree protections will be afforded, and who is privileged to access protected items. A policy is influenced by:

1. The functional requirements of an information system (what users need to accomplish from the system)
2. The security requirements for the system (items that need to be protected)
3. A threat model (the expected motives and resources of potential perpetrators).

SOLUTION:

Threat models should consider potential "attacks," whether accidental or intentional, on the integrity and availability of health data. Hard­ ware or software failures, including "denial-of-ser­ vice" attacks, can cause downtime or loss of vital health care data for EMR users. The reliability of EMR systems and data should be considered a security concern and should be covered in security policy and system management activities, usually through mechanisms that support data redundancy and system backups.

Electronic patient data can be asswned valid based on software testing and verification, access-control mechanisms, and error-checking protocols used in data transport, or they can be additionally authenticated as valid with digital signatures, as discussed above. Most lapses in data integrity will continue to be due to human error and to malfunctions or ''bugs" in medical computer systems.

Firewalls are computers that are positioned between a site's internal network and an unsecured public net­ work, such as the Internet, and may be useful at EMR sites. Firewall computers are configured to monitor and regulate the messages passing into and out of a site's private network and so can prevent unauthorized users from entering local computer systems from the outside, or can prevent particular programs and services from operating through the firewall.