

### EMIS Users FAQ #3

#### How is security and confidentiality handled in EMIS?

1. MDERA physicians requested shared EMIS patient records common to all MDERA physicians.

Example: In the case of group practice, a physician caring for another physician's patient can access that patient's complete chart using their own user ID and password.

2. Another level of security can be accessed in EMIS by individual physicians and applied to specific patient records; thereby rendering patient information entered by that physician inaccessible to others. (For instructions on how to access this level of security, select EMIS Training handout: PCS Configuring Confidentiality Policies.)

Example: a) A physician may wish to prevent patient information, entered by that physician, from being viewed by others. This physician can select this level of security for specific patients at the time of information entry. A Confidential notice will appear.

b) Another physician may be required to provide urgent care for these specific patients. That physician would, therefore, need to access the secured patient information. They can do so by "breaking the glass" as described in point # 3. below.

3. A break the glass option exists to be used only in an urgent situation with a patient.

This allows the attending physician to access the previously secured information.

Example: The attending physician may reverse the Confidentiality status of a patient's information. This change in status will occur for the attending physician only – not for all EMIS users. The physician will be required to give the reason for breaking the glass; it will trigger an audit trail.

#### Who can access patient information in EMIS?

In EMIS security profiles are assigned by the type of work each staff person performs. Only the access each individual needs to conduct their work is provided. The login screen for individuals with differing access will look different because modules to which they do not have access will not be on their screen. EMIS automatically creates an audit trail of who accessed which information on a specific date and time. An audit report can be generated for monitoring purposes.