

Data security is of utmost importance in the world today. Protecting your information from HIPAA or FERPA violations should be a top priority. ATS allows access for multiple users, with a unique login and strong password to the information given to them by the ATS system administrator.

Meaning that, coaches, staff, or anyone else with a log in, only sees the information granted permission to view. If you have multiple schools under one umbrella of an organization, personal information does not fall on the eyes of anyone who should not see it.

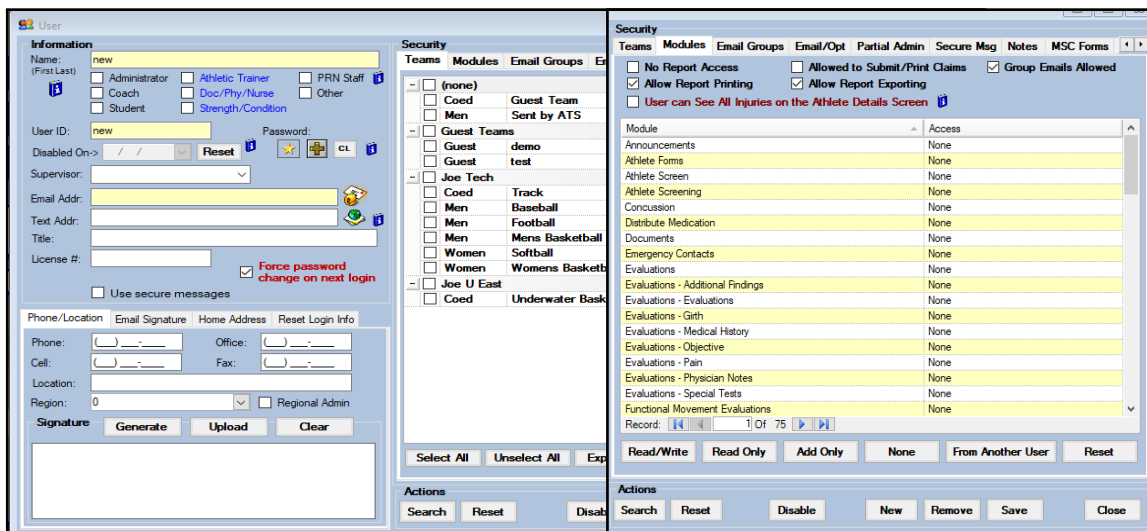
**Definition of Terms used in ATS pertaining to access:**

**Patient/Athlete**— a person that does not have staff access to the Desktop, or Staff Portal. They access the system through the Patient Phone, Patient Portal or Kiosk. They are required to have a sign in ID and Password to access only their information.

**Emergency Contact**— a person that does not have staff access to the Desktop, or Staff Portal. They access the system through the Patient Phone, Patient Portal or Family communication center. They can be tied to specific athletes, register their athlete, update information. They also must have their own sign in ID as well as password.

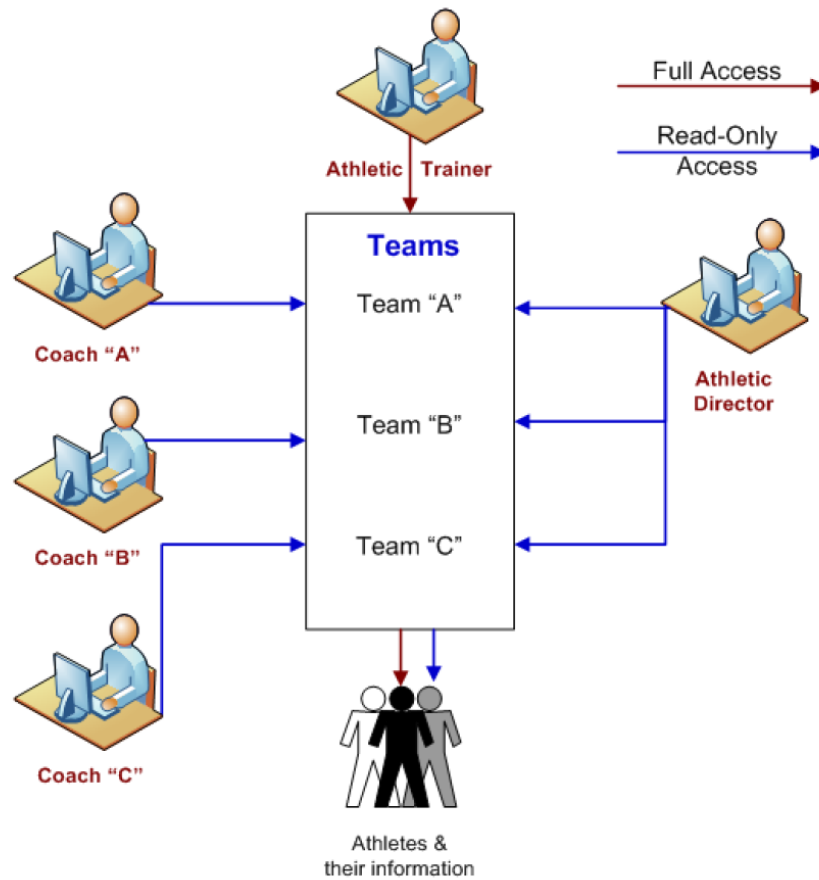
**USER**— Anyone in ATS that will access through the Desktop, Staff Portal or Staff Phone. This can be, athletic trainers, physicians, physician offices, insurance coordinators, coaches, athletic directors, school nurse, or athletic training students. Access is granted for specific information and controlled by the system administrator. You control their ability to **read/write** information (see and enter), **read only** (see only), **add only**( only able to add information, not able to see anything that has been added prior), or **none** access, so they do not see any information associated. You also control the access to teams, if they are not checked off to “see” a team, they will never know that it exists.

Below is an example of the new user profile. Everything begins blank, so you must grant access to all of the appropriate areas for the new user. If you do not configure the account, they will be able to log in, but will never see any information. For more information see the [User Configuration](#), or [Coach Configuration](#) help docs.



Below are flow charts showing the way information can be shared, and who is able to see and access information.

The image below, is detailing a simpler configuration. Showing coaches have access to their respective teams, the Athletic Trainer has full system access, controlling what they can see. The athletic director is only able to see information for all athletes/teams, but not edit anything within the system.



This image is showing more of a “region” or supervising athletic trainer. They see the ATs underneath them, the athletic trainers only see their schools information, even though there are four under the one umbrella organization. Coaches would work as illustrated above, only seeing their information, under the school they work for. Only the person in charge, is able to see all information.

