



eCornerstone

www.iphca.org/eCornerstone/implement.htm

Confidentiality Issues and eCornerstone

Guarding the identity of human services customers is an important principle of the Cornerstone and eCornerstone systems. Procedural and technological protections within both systems prevent the release of confidential information. In fact, since the beginning of Cornerstone in 1997, there has been no known breach of a customer's confidential information. The purpose of this bulletin is to review the procedures and technology used by eCornerstone to guard the identity of youth services recipients.

A critical consideration underlying the consent process for eCornerstone is that the youth services contracted for by the Bureau of Youth Services and Delinquency Prevention, Division of Community Health and Prevention, do not include mental health or developmental disabilities services. However, many providers under contract to provide youth services also provide mental health or developmental services through other contractual arrangements. eCornerstone contains information specific only to the Bureau of Youth Services and Delinquency Prevention programs.

An eCornerstone Informed Consent form is to be completed and signed for every recipient who is new to an eCornerstone agency. This includes recipients who are new to the agency either through transfer or referral. The form must be signed by the participant or his/her legally authorized parent or guardian. One eCornerstone Informed Consent form is required per participant per agency, regardless of program participation.

Consent gives the agency permission to share the following information about the participant to other service providers: program enrollment and assessment results or scores. Consent does not authorize the release of answers to assessment questions, progress notes, and case worker assignments. This information is considered confidential. eCornerstone prevents this information from being shared with any other service provider beyond the agency of participant intake.

Because the majority of program recipients are not of an age to consent to sharing their information, eCornerstone has built in protections to enable the youth services provider to enter program related data without allowing it to be shared with any other service provider until a parent or guardian agrees. This system protection allows service providers to comply with program reporting requirements independent of consent. eCornerstone requires the service provider to designate early in the data collection process whether a consent form was signed. In the event of no consent, eCornerstone will flag the recipient's program related data to prevent it from being shared beyond the agency of origin.

Many technologies are being relied upon to protect confidentiality, including firewall technology. The security in place is likened to security found in online banking and online shopping applications. The eCornerstone system requires the use of a log-in name and password, which enables an encrypting mechanism. Therefore, all information that travels from the provider to the Central Office in Springfield will be encrypted, rendering it unreadable to a third party.

With all of the above considerations and safeguards, there is a high degree of confidence that our clients' identities will remain protected by the system that will be so critically important in the provision of high-quality services.