SECURITY BREACH POLICIES & PROCEDURES

The Policies and Procedures for managing the security breach of PII (Personally Identifiable Information) data in the HMIS apply to all Bakersfield-Kern Reginal Homeless collaborative members and Kern County HMIS end users. The following document will outline the process that the HMIS Committee members will use to respond to the HMIS security breaches.

Policy

To manage the data security in the HMIS and the database at the agency level, the following procedures have been taken place to respond the incidents (such as security breach or privacy breach, unauthorized access, sharing of HMIS user id/passwords, and many more as described in the HMIS Data Quality Policies &Procedures Manual). The following document will address how the HMIS lead will respond to any incident, like Unauthorized person access to clients PII, Sharing HMIS Login information, Loss of client's confidentiality data, Theft or loss of any client physical detailed/hardcopy form, unauthorized transfer of client data, Misuse of client details, Theft or Loss of hardware including computer, storage hard drives, unusual activity at the system level and many more but not limited to.

Procedures

The following information describes what will happen once any breach has occurred:

1. The HMIS user will directly address the issue to the HMIS Data Supervisor/Administrator at the agency. The Breach can be discovered or suspected by any HMIS user, Data Administrator, or HMIS Lead when someone suspects that something is "not right", or "unusual activity" occurred within the system.
2. The higher authorities at the agency, the HMIS Data supervisor/Administrator will directly report the issues to the HMIS lead.
3. The HMIS Lead will investigate the Breach and document the incident details.
4. The HMIS Lead will inactivate the suspected user's login immediately.
5. The HMIS Lead will monitor the details of the affected and compromised client.
6. The HMIS Lead will investigate on nature of the breach that occurred accidentally or intentionally.
7. If the incident level threatened many clients' detail and agency data then the HMIS lead can temporarily inactive or disable access for a partnered agency, for a particular project type, or maybe specific to some count of end users.
8. The HMIS lead will discuss or execute the action plan along with the Partnered agency members to resolve the incident.
9. The HMIS Lead may notify the HMIS Governing body about a breach of data that occurred at the partnered agency and action plan taken to take care of it.
10. The HMIS lead may ask partnered agency's end users to complete the HMIS user training and sign the End user agreement once again.
11. If the Breach has occurred at the agency level, then the HMIS lead will revoke the end user license permanently.
12. And if the breach has occurred at the agency level involving a group of end users, then the HMIS lead/ Data Security officer will notify the appropriate body of the Continuum of Care or the HMISHMIS Governing Body.