LOUISIANA HEALTH CARE QUALITY FORUM

POLICY: Physical Security of Hardware, Data, Media and Equipment	**EFFECTIVE: 10-01-2011**
DEPARTMENT: LHCQF; LaHIE	**REVISED:**

PURPOSE

To facilitate compliance with all applicable laws and regulations regarding the system security, including, at a minimum (a) meeting the standards established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) pertaining to system security and workstation security and (b) complying with the security provisions of this Policy Manual with respect to the hardware and systems used by the Louisiana Health Care Quality Forum (LHCQF) and in connection with the Exchange (LaHIE).

RESPONSIBILITY

LHCQF's Health IT Director or his/her designee shall act as the Security Officer and ensure that LHCQF/LaHIE complies with all applicable laws and regulations regarding the system security and physical security of the hardware, data, media and equipment utilized by the Louisiana Health Care Quality Forum and LaHIE.

Participants of LaHIE shall comply with all applicable laws and regulations regarding system security, including at a minimum, (a) meeting the standards established by HIPAA pertaining to system security and workstation security and (b) maintaining the security of the workstations through which their Authorized Users access LaHIE.

LHCQF's Health IT Director or his/her designee shall ensure that the Exchange's (LaHIE's) technology vendor maintains the security of the hardware located in the vendor's data center (the "Data Center") as well as the hardware maintained by LHCQF staff, i.e. laptops.

PROCESS

1. LaHIE, Participants and all vendors will comply with, the following system security standards:
    a. To protect the confidentiality, integrity and availability of LaHIE by taking the reasonable steps to protect hardware used in connection with LaHIE, as well as the facilities in which it is located, from unauthorized physical access, tampering and theft.
    b. To physically locate hardware used in connection with LaHIE in locations where physical access can be controlled in order to minimize the risk of unauthorized access.
    c. To take reasonable steps to ensure that the perimeter of facilities containing hardware used in connection with LaHIE is physically sound, the external walls are properly constructed and the external doors have the appropriate protections against unauthorized access.
    d. To prevent against unauthorized access to the facilities at which hardware used in connection with LaHIE is located by ensuring that doors and windows of all facilities are locked when unattended and that external protections, such as window guards or bars, are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.
    e. To establish and document detailed rules to determine which workforce members are granted physical access rights to specific areas where hardware used in connection with LaHIE is maintained and to provide such physical access rights to the work area only to

workforce members having a need for access to such an area in order to complete job responsibilities.

2. Data Center Security Standards
    a. To use the following controls at all delivery and loading areas to prevent unauthorized access to its facilities:
        i. Restrict access to a holding area from outside building to identified and authorized workforce members
        ii. Design the holding area so supplies can be unloaded without the delivery staff gaining access to other areas of the building.
        iii. Secure the external doors of the holding area when the internal door of the area is open.
    b. To take reasonable steps to ensure that the level of protection provided for LaHIE, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks to the security of LaHIE and its facilities.
3. Periodic risk analysis will be performed by LHCQF's Health IT Director or his/her designee in order to assess the level of physical access risk and adjust procedures accordingly.
4. LHCQF's staff laptops will not contain unencrypted PHI on the hard drive.

APPROVAL:
Cindy Munn
Executive Director
Louisiana Health Care Quality Forum