PRIVACY & SECURITY INFORMATION NOTICE

RAISING AWARENESS ABOUT THE IMPORTANCE OF PROTECTING THE PRIVACY & SECURITY OF SENSITIVE INFORMATION

County Information Security Guidelines **06/17/08**

Careful consideration must be taken when removing County information (whether it is in paper or electronic format) from the safeguards of the County Network and its building/facilities. The responsibility of protecting County information transfers over to you when you remove it from the County's protection. Will you be able to provide the same level of protection as the County? Have you obtained manager/supervisor approval to take such information home?

Removing restricted, confidential, and/or sensitive information such as client/patient records, financial records, personnel records from County safeguards is highly discouraged. However, when a business need arises to do so, the following guidelines are reasonable precautions to follow for protecting this type of County information (these guidelines are not all inclusive). **You must first obtain approval from your manager/supervisor before taking such information out of the County's protection. Keep track of the information you remove.**

Paper documents:

- Carry documents in a folder or briefcase.
- Do not leave documents in view of others to see or where it can be easily accessible to others. When working out in the field (e.g. site/home visits), carry the folder or briefcase with you. When it is not feasible to do so, keep the documents out of sight and secure your vehicle. Check to make sure the documents are still there when you return.
- Upon returning to the office or your home, remove all documents from your vehicle - do not leave them inside the vehicle. Keep the documents in a secure home location if you are not returning to the office.

Mobile storage media:

- County information must **only** be stored on County purchased storage media, such as CDs, floppy disks, flash drives, etc.
- Keep storage media in a secured place, such as in a locked drawer or filing cabinet when not in use.
- Encrypt and Password-protect the file(s) on the media to provide a two-layer level of protection.
- Do not save County information in personally owned media or devices including the hard drive of your personal computer.

Mobile devices/equipment:

- County information must **only** be stored on County purchased or leased mobile devices, such as laptops, PDAs, Blackberries, PC Tablets, etc. Do not store information on the 'C' Drive (hard drive) unless encrypted and password protected when necessary.
- Remove the device from your vehicle - do not leave it inside when not in use. When working out in the field, take the device with you. When it is not feasible to do so, keep the device out of sight and secure your vehicle. Check to make sure it is still there when you return. When you do take the device with you, do not leave it unattended at the location you are visiting so that it is not left behind or forgotten.
- Keep the device stored in a secured place, such as a locked drawer or filing cabinet when not in use. Place the device in a secured home location where it cannot be easily accessible to others if you are not returning to the office.
- Remove the laptop from its docking station unless it is physically secured with a cable lock.

Take extra precaution with paper documents, storage media and/or mobile devices that contain a person's information (e.g. SSN, DOB, home address).
Immediately report any lost or stolen information to your manager/supervisor.

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT:
Pilar Miranda, HHSA Information Security Manager
(619) 338-2806
Pilar.Miranda@sdcounty.ca.gov

HHSA Information Technology Division