Policy #52

Privacy, removable media, remote access, and personal mobile devices

This policy applies to all media in any format that contains confidential information including protected health information (PHI); financial, banking and legal information; taxpayer information including social security numbers; and any other information made confidential by law or St. Clair County's policies (the "Confidential Information"). Prevention of unauthorized access to Confidential Information held by St. Clair County (the "County") will be maintained by controlling the use, re-use, storage and disposal of media containing such information, as well as access to such information.

The purpose of this policy is to ensure that Confidential Information is protected from unauthorized access and disclosure and to comply with applicable laws, including, but not limited to, the privacy and security provisions of the Health Insurance Portability and Accountability Act (HIPAA) to the extent the same regulates activities of St. Clair County.

Media which may contain protected or confidential information may include, but is not limited to:

- Paper documents such as medical records, billing records, FMLA applications, workman's compensation filings, documents wherein an individual's social security number is included, etc.
- Documents, notes, or the like containing Confidential Information
- Photographs and/or overhead transparencies of or related to Confidential Information
- Electronic media such as computers, personal digital assistants, digital recorders, or any other handheld or wireless device; removable magnetic media such as CD, DVD, optical disk, Zip disk, portable hard drive, flash drive, audiotape/videotape, etc.

All media containing Confidential Information should be handled in a manner so as to prohibit unauthorized access and/or dissemination. Complete removal of Confidential Information from media is required before the media is made available for re-use. When the use or retention period of any media containing Confidential Information is completed, the Confidential Information must be destroyed, rendered unrecoverable, or returned to the owner.

Other related policies: St. Clair County Policies #16 and #34

Access to and disclosure of Confidential Information will be monitored by the County Administrator and the Privacy Officer. Employees in need of access to Confidential Information shall first make the request to the County Administrator and shall not be granted such access unless and until the County Administrator determines said requested access is necessary.

Those requiring remote access to County servers or software of any type must be approved by the County Administrator and St. Clair County Technology Cooperative. Remote access to financial software/information may be granted to certain specific employees; however, **at no time will remote access be granted for payroll or personnel software/information and/or personnel health care or medical related information.** Computers, hardware, and other devices used to remotely access Confidential Information shall be property of St. Clair County and shall be 'prepared' by the Technology Cooperative. At no time shall an employee or any other individual gain remote access to County servers, software, or other property which might provide access to Confidential Information using personally owned computers or devices.

Confidential Information is not to be stored or "backed up" onto removable media at any time. St. Clair County supports off-site server back-up for this purpose.

Confidential information shall not, under any circumstances, be recorded, photographed or otherwise documented or copied by an employee's personal media, storage or wireless devices. This includes personal computers, cameras, voice recorders, tablets, cell phones, etc.

Adopted this day ____Nov. 12, 2013_____