



Policy Number: 51
Effective: August 11, 2026
Revised: N/A

Subject: Cell Phones

PURPOSE:

Camden County Developmental Disability Resources (CCDDR) shall have a policy that pertains to the CCDDR issued cell phones and, when necessary, the use of personal cell phones for CCDDR business. This policy describes the acceptable use of cell phones as well as the unauthorized uses. Cell phones can be a valuable tool for Support Coordinators and other staff but should be utilized within specific guidelines to ensure the protection of client rights, employee rights, confidentiality, privacy, CCDDR, and the Board of Directors.

DEFINITIONS:

Protected Health Information (PHI): PHI is any health information that can identify a current or previous CCDDR client's past, present, or future health. This data also includes, but is not limited to, demographic information, record numbers, names, initials, addresses, phone numbers, emails, and biometric information, such as fingerprints, voiceprints, genetic information, and facial images.

Health Insurance Portability and Accountability Act (HIPAA) Compliant: The guarantee that an agency, information system, or software provides adequate protection as defined by law to the handling of PHI.

Confidential Employee Information: Information about a current or previous CCDDR employee that includes personal identifying details including, but not limited to, social security numbers, home addresses, dates of birth, disciplinary actions, performance reviews, background checks, accommodation requests, disability status, and medical details.

POLICY:

CCDDR issues its employees a cell phone that is owned and managed by CCDDR. CCDDR uses professional account management software that allows CCDDR to remotely enable, disable, and "wipe" (return phone to factory defaults) each CCDDR issued phone. This program also allows CCDDR to prohibit unauthorized software applications from being downloaded and internet sites from being accessed.

The CCDDR issued cell phone is to be used for CCDDR business purposes only. Employees should always turn off or silence any CCDDR issued or personal cell phone when asked to do so. In some situations, the Compliance Director or Executive Director may authorize the use of the CCDDR issued cell phone that would normally be considered unauthorized use or an employee's personal cell phone if a CCDDR issued cell phone is not operable or available. Such use may be necessary to preserve or continue effective CCDDR operations or to protect the safety, security, or well-being of a CCDDR client or employee, so long as the use does not violate Federal, state, or local laws. Unauthorized use of a CCDDR issued cell phone includes, but is not limited to:

- Making personal calls or texts
- Downloading/Playing games
- Downloading/Playing music
- Downloading/Playing/Watching videos not related to the employee's job responsibilities
- Accessing personal email
- Sending texts that contain PHI or confidential employee information without the use of CCDDR approved HIPAA-compliant encryption software for texting (this applies to personal cell phones approved to be used for CCDDR business as well)
- Including PHI or confidential employee information in phone call conversations where any unauthorized person(s) and/or the public can hear the conversation (this applies to personal cell phones approved to be used for CCDDR business as well)
- Accessing CCDDR SharePoint files, CCDDR OneDrive files, CCDDR's accounting database, CCDDR's TCM database, state owned/operated databases containing PHI (e.g. CIMOR, ConneXion, Mo HealthNet, etc.), and/or provider owned/operated databases containing PHI (this applies to personal cell phones approved to be used for CCDDR business as well)
- Accessing/Utilizing unauthorized software, databases, internet sites, social media sites, and/or other services
- Using for any reason while driving that violates state or local laws unless using hands-free or voice-operated communication methods acceptable under state or local laws (this applies to personal cell phones approved to be used for CCDDR business as well)
- Using the camera or microphone to record PHI or confidential employee information, unless the client/guardian or employee has provided written consent/approval to do so; however, the recorded information obtained must be immediately transferred to the appropriate CCDDR database or file and then immediately deleted from the cell phone after transfer (this applies to personal cell phones approved to be used for CCDDR business as well)
- Using in locations where cell phone use is explicitly prohibited (e.g. laboratories, courtrooms, etc. – this applies to personal cell phones approved to be used for CCDDR business as well)
- Downloading, uploading, texting, messaging, emailing, and/or storing/saving inappropriate, illegal, or obscene material (this applies to personal cell phones approved to be used for CCDDR business as well)
- Using in the commission of a crime or while carrying out illegal activity (this applies to personal cell phones approved to be used for CCDDR business as well)

Employees are expected to immediately report any damage to, malfunction of, or loss of the CCDDR issued cell phone to their supervisor, the Compliance Director, and/or the Executive Director. If it is determined that the damage, malfunction, or loss was due to any purposeful action of an employee, CCDDR may ask for restitution, and disciplinary action, up to and including termination, may be administered.

CCDDR retains the right to monitor employees for excessive or inappropriate use of a cell phone. Examples that may result in disciplinary action, up to and including termination, include, but are not limited to:

- Causing a security breach
- Violating this policy
- Violating other CCDDR policies and/or procedures
- Violating HIPAA laws/regulations

- Causing an accident by recklessly using the cell phone
- Using a CCDDR issued cell phone for personal business

CCDDR expects its employees to use their CCDDR issued cell phones prudently during working hours. When working remotely, the CCDDR cell phone should be used for all agency related communications when the use of a cell phone is necessary. Authorized activities also include installing CCDDR approved agency email platforms, installing CCDDR approved software, and accessing the internet to assist or inform clients/guardians. In the event personal cell phone use is authorized because a CCDDR issued cell phone is not operable or available and is necessary for continuing effective CCDDR operations, CCDDR may require the employee to temporarily install CCDDR approved agency email platforms and software. CCDDR will pay for any costs associated with temporarily installing CCDDR approved email platforms and software on a personal cell phone, and the employee will be reimbursed the approved CCDDR monthly reimbursement rate after submission of a monthly expense reimbursement form. The monthly reimbursement rate may be prorated based on the number of days the personal cell phone was used for CCDDR business purposes during any month.

REFERENCE:

- CARF Standards Manual