Guidance for CASA/GAL Programs

MAINTAINING CONFIDENTIALITY IN THE MIDST OF DISRUPTED OPERATIONS

CASA GAL
Court Appointed Special Advocates
Guardians ad Litem
FOR CHILDREN
NATIONAL CASA/GAL ASSOCIATION

We are providing guidance on a number of program and volunteer functions in light of the coronavirus (COVID – 19). The National CASA/GAL Standards (Standards for Local CASA/GAL Programs 2012 version - Standards 2.B.1 – 2.B.9) for maintaining confidentiality remain in effect even when authorities issue stay-at-home, shelter-in-place, or other orders disrupting operations. As programs may face disruptions to their normal practices of communicating and storing confidential information, this document provides guidance and clarification on acceptable practices while the COVID-19 pandemic persists. At all times, state, local, and tribal law and direction from relevant authorities shall take precedence over guidance from National CASA/GAL.

SHARING CONFIDENTIAL INFORMATION

Phone Calls and Video Conferencing. With families sharing work spaces in their homes, finding a private place for a phone conversation or video conference can prove difficult. Therefore, staff and volunteers should not share confidential information with other staff over the phone or in a video conference unless they have confirmed that no one else can hear the conversation (on either side of the call). If callers cannot find a quiet, private location inside their home, they might consider going inside a car.

Text. Staff and volunteers should not share confidential information via text because of the inherent lack of security in text messaging and because those communications are discoverable.

E-mail. If sharing confidential information via e-mail, make sure to use encryption. Never share confidential information using personal e-mail accounts.

SIGNING STATEMENTS OF CONFIDENTIALITY

The standards (Standards 2.B.3 and 2.B.4) regarding volunteers and staff signing statements of confidentiality remain in effect. However, staff do not need to collect those signatures in person, but may use electronic signatures, scan signed documents with their smartphone, or mail documents.

MAINTAINING CASE FILES, UP-TO-DATE AND SECURE

The standards (e.g., Standards 2.B.6, 2.B.7, 2.B.8, 11.A.1, 11.A.2, 11.A.3, and 11.A.4) about maintaining complete, accurate, and current case records, including keeping confidential information safe and secure, remain in effect. This does not mean that programs must maintain files in the same ways that they did before staff had to start working from home, but programs need to implement adequate security for these records. Additionally, programs continue to need to ensure that they have controls in place that allow staff to locate these records at any time.

Electronic records. Staff should not store confidential records on their personal computers or on the local (C:) drive of a work computer. They should upload records to the case management system or the program's shared drive. In the event recording-keeping practices change in response to the COVID-19 pandemic, the program should issue written guidance so that all staff follow the same practices for storing confidential records. Upon

resumption of normal operations, staff should move the records to the place where they would normally store it, and delete the record from the temporary location.

Physical records. Programs should maintain logs of any physical records that staff keep at their homes. Each program should keep the log on a shared drive so that all staff have access to it. Staff should lock all confidential records that they keep at their homes – in a cabinet, a home office, or their car in a locked, private garage. Staff should not leave any confidential records in a car parked on the street or in a shared garage.