



Updated: January 15, 2025

Responses to Subpoenas and Court Orders (U.S. Only)

The following terms apply when we (AppClose, Inc.) receive a request to produce documentation of records on our apps. A user may always export/download their own records from the app without charge. A legal or other professional registered with [AppClose Pro](#) may download certain client co-parent records with the consent of the co-parent. Using AppClose Pro, a legal professional may also create evidence summaries with records attached, which summaries are often allowed in pre-trial proceedings in family law courts.

If a certified Business Records Affidavit with records attached is required for court proceedings, we must first receive a valid subpoena as described below.

AppClose® complies with all valid subpoenas and court orders to produce records that comply with the Texas Rules of Civil Procedure, or other applicable procedural or substantive rules. AppClose will follow Texas law unless we are otherwise required by other laws that may apply to us in litigation or with respect to law enforcement. To determine our legal obligations and the appropriate response, we reserve the right to evaluate each individual request.

The Uniform Interstate Depositions and Discovery Act (“UIDDA”) is not yet effective in Texas.¹ AppClose will generally accept a subpoena for records from or through an out of state court if the requirements in this policy are followed. Unless and until the UIDDA becomes effective in Texas, AppClose reserves the right in its sole discretion to require that a subpoena be issued and served through a Texas court under the Texas Rules of Civil Procedure. Due to privacy concerns about Adverse Party Records (as defined below), unless and until the UIDDA is effective in Texas, subpoenas that request Adverse Party Records will require additional procedures, and are more likely to require issuance and service through a Texas court under the Texas Rules of Civil Procedure.

Our general policy for subpoenas requires the following:

- (a) A valid subpoena issued and served under the Texas Rules of Civil Procedure; (b) an out of state subpoena otherwise accepted by AppClose as described in this policy; or (c) a valid summons, search warrant, or subpoena from law enforcement.
- A civil subpoena MUST be accompanied by a HIPAA compliant authorization signed by the requesting co-parent to release, for the purpose of responding to the subpoena, any protected health information that may be contained in such parent’s records. The HIPAA compliant authorization must cover the parent requesting the records, as well as all children entered in the App. A form of HIPAA compliant authorization is attached.

¹ The UIDDA was signed into law in Texas effective September 1, 2023, but it will not be effective in Texas unless and until it has been adopted by the Supreme Court of Texas. The Supreme Court of Texas has until September 1, 2025, to adopt the UIDDA, failing which, the existing process in Texas would remain in effect. The Texas Supreme Court has asked the Texas Supreme Court Advisory Committee to begin work on the UIDDA. Texas has adopted the Uniform Act to Secure Attendance of Witnesses From Without State. See Texas Code of Criminal Procedure, Art. 24.28. Any subpoena or order issued under that act, or the Stored Communications Act (18 U.S. Code § 2701 *et seq.*), is beyond the scope of this subpoena policy.

- We use our own form of Business Records Affidavit, which is based upon the manner in which our records are created, stored, and maintained.
- Each subpoena MUST identify the email that is associated with the account for which records are requested. We do not associate a person's name or DOB with their account.
- We do not currently charge a subpoena response fee.
- When responding to a valid subpoena or court order, AppClose' authorized technical personnel unencrypt and compile the specific data within the date range described in the subpoena or court order. AppClose **does not** screen or otherwise review the contents of the unencrypted data.

Should you wish to contact us about requesting records, you will be directed to this policy and advised to produce a valid subpoena, court order, and other appropriate documents described above. We are a Delaware corporation, with our principal executive offices in Austin, Texas. We are registered to do business in Texas. Our records are maintained by our principal executive office in Austin. Our agent for service of process in Texas is Igor Litinsky, 5000 PLAZA ON THE LAKE STE 300 AUSTIN TX 78746.

You may e-mail a pdf of the subpoena or court order to legal@appclose.com. E-mail of a subpoena will not of itself constitute service of the subpoena. AppClose may **voluntarily and in its sole discretion** accept service of an e-mailed subpoena. Acceptance of any such e-mailed subpoena is more likely if the subpoena and/or other communications (a) meet the requirements of this subpoena policy, including the identification of the email address associated with the account for which records are requested; (b) includes (or timely provides) the required signed HIPAA authorization(s); (c) clearly describe the records requested (including the date range) from the list of "Records Maintained" below; (d) clearly state that the subpoena seeks only the production of documents and/or records, and not the appearance of AppClose personnel at any legal proceeding related to the subpoena; and (e) specify an email address to which the Business Records Affidavit may be emailed.

In connection with information provided in response to a subpoena or court order, AppClose makes no warranties, representations, statements, or guarantees (whether express or implied) regarding the material and information transmitted or to provide any updates to information transmitted. AppClose provides records within the date range(s) requested in the subpoena. We do not search the records for specific terms, or review the records in any respect. Records may be downloaded by a user or legal professional (with the user's consent) in pdf format may be searched by such user or legal professional using applicable pdf search capabilities.

Policy Regarding PII and Adverse Party Records for Civil Subpoenas

A subpoena must identify the account (email address) of the co-parent requesting the records. The records associated with that account will **automatically include all communications from the other co-parent to the requesting co-parent**.

Absent a court order signed by a judge, proof of a court-approved confidentiality agreement or protective order for the benefit of the adverse party, or other assurances satisfactory to AppClose in its sole discretion that the adverse party has been notified of the subpoena request and has had the opportunity to seek a confidentiality agreement or protective order, we will **not** produce records or PII (such as telephone numbers or email addresses) that are **unique** to the non-requesting co-parent's account ("**Adverse Party Records**").

AppClose is an out of state nonparty to subpoenas. For an out of state subpoena, as noted above, the UIDDA is not yet effective in Texas. AppClose reserves the right to require that any out of state civil subpoena be issued through a Texas court, particularly for subpoenas that request Adverse Party Records and that do not satisfy all of the above requirements for subpoenas that request Adverse Party Records.

Records Maintained

Currently, we maintain the following records:

- chat conversations (including images)
- call detail records (but **not** call recordings or call transcripts)
- check-ins, expenses, and requests
- session logs (which include the time, IP address, and mobile device operating system)²

Each subpoena should identify (a) the specific types of records sought from the list above; and (b) the time period for which the records are sought. As noted, we use the email address associated with an account to identify each account (some users **optionally** provide phone numbers).

PII Not Maintained

We do NOT maintain other personally identifiable information, including any of the following:

- Device IDs
- Geolocation data
- Social security number, driver's license number, or passport number
- Postal street address
- Bank account numbers

² Note that the IP address associated with a mobile device is not permanent or unique, and can vary depending on the network to which the device is connected at any given time. We do not track device IDs. An IP address does not determine the actual person interacting with an account.