



Updated: October 1, 2026

AppClose Certified Records and Subpoena Policy

IN LIEU OF SUBMITTING A SUBPOENA, USERS MAY DOWNLOAD CERTIFIED ELECTRONIC BUSINESS RECORDS, WHICH WILL IN MOST CASES BE THE FASTEST AND MOST EFFICIENT WAY TO OBTAIN CERTIFIED BUSINESS RECORDS FOR EVIDENTIARY PURPOSES

A. TYPES OF RECORDS AVAILABLE

- 1. Uncertificated Records.** AppClose users may at any time and from time to time log in to their account and export records defined as Exportable Records in the Terms of Service ("Exportable Records"). These records include communications between that user and other users with which the user is connected in AppClose, as well as other activity within AppClose **by that user**. These records can be shared **at the user's discretion** with third parties, including the user's attorney and/or a court. Uncertificated records may not be accepted for admissibility in many types of court proceedings. AppClose certified records are available when user records are required for evidentiary purposes. Final decisions on admissibility are determined by the appropriate court.
- 2. Certified Records.** For user records, AppClose offers two types of certified records, each designed to satisfy the evidentiary rules described in this Policy:
 - a. Certified Electronic Business Records:** any U.S. user may initiate an export of their own Exportable Records in the form of Certified Electronic Business Records. AppClose Certified Electronic Business Records are designed to be offered in evidence without testimony from a records custodian. The Certification described in Part B states, under penalty of perjury, the facts required by the business-records exception to the rule against hearsay. That exception is recognized in every state and in Federal Rule of Evidence 803(6), and in most jurisdictions the foundation may be established by a custodian's certification or affidavit rather than by live testimony — in Texas, under Rule 902(10) of the Texas Rules of Evidence, and in federal court, under Federal Rule of Evidence 902(11). Certified Electronic Business Records are also built to meet Federal Rules of Evidence 902(13) and 902(14), which address records generated by an electronic process and data authenticated by digital identification, in jurisdictions that have adopted those rules or their counterparts. A Certified Electronic Business Records export is a PDF file that contains the exported records together with the Certification described in Part B, signed electronically by the AppClose Custodian of Records. The PDF file as a whole is also signed with the digital signature of AppClose, Inc., issued by a certificate authority that is a member of the Adobe Approved Trust List, and a trusted timestamp, both applied automatically when the export is generated. The digital signature identifies AppClose as the source of the file and reveals any alteration made to the file after it was signed, and it can be verified in ordinary PDF software without contacting AppClose. The Certified Electronic Business Records may be provided by a user to the user's attorney or other third party either by (i) the user sending a pdf (or link to the records export) directly to their attorney or other third party, or (ii) by the user giving their attorney electronic consent in AppClose for their attorney and/or the court to access the records export directly through *AppClose Pro*. This process is described in more detail below.
 - b. Business Records Affidavits in response to proper Subpoenas.** While Certified Electronic Business Records are more efficient, faster, more secure, and verifiable as to origin and integrity

UNITED STATES

by anyone who receives them, as described in Part B, AppClose will still provide Certified Business Records Affidavits in response to a proper subpoena. AppClose complies with all valid subpoenas and court orders to produce user 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 subpoena process is described in more detail below. Our Business Records Affidavit is signed by our Custodian of Records as an unsworn declaration made under penalty of perjury. In most instances an unsworn declaration under penalty of perjury is admissible in place of a sworn affidavit, including under Federal Rule of Evidence 902(11) and 28 U.S.C. § 1746 and, in Texas, under Texas Rule of Evidence 902(10) and Section 132.001 of the Texas Civil Practice and Remedies Code. If a notarized affidavit sworn before a notary public is required or preferred in your proceeding, we will provide one on request. Please make that request in your subpoena or in your cover communication so that we can accommodate it within the processing time described below. We do not charge any fee to provide Business Records Affidavits.

3. **Charges for Records.** We do not impose any additional charges or fees to provide records – unlimited access to a user’s own records is available to every user. If a user’s Account is in Read-Only Mode (as that term is defined in our Terms of Service), the user can still sign in, view their records, and export all of the records in the Account at any time, including by requesting Certified Records.
4. **Closed Accounts.** A user cannot sign in to a Closed Account (as that term is defined in our Terms of Service), so a Certified Electronic Business Records export cannot be initiated from a Closed Account. In the United States, certified records for a Closed Account are available through this Policy, by a Business Records Affidavit issued in response to a proper subpoena or court order as described in Part C below. A former user who needs an uncertified copy of their records should follow the process described in our Terms of Service, under which we deliver a pdf of the exportable records to the email address associated with the Closed Account.

B. APPCLOSE CERTIFIED ELECTRONIC BUSINESS RECORDS.

1. **Purpose of AppClose Certified Electronic Business Records.** AppClose Certified Electronic Business Records (“CEBR”) are designed to establish the business-records foundation on the face of the export, so that the records may be offered without testimony from a records custodian. The business-records exception to the rule against hearsay is recognized in every state and in Federal Rule of Evidence 803(6), and most jurisdictions allow that foundation to be laid by a custodian’s certification or affidavit in place of live testimony (in Texas, Rule 902(10) of the Texas Rules of Evidence; in federal court, Rule 902(11)). CEBR are also designed to meet Federal Rules of Evidence 902(13) and 902(14) in jurisdictions that have adopted those rules or their counterparts. When AppClose user records are needed for evidence, AppClose CEBR should in many cases eliminate the need for a records subpoena.¹ Since an AppClose CEBR can be issued within minutes, it saves the time and expense associated with the issuance of a records subpoena, as described below under “Business Records Affidavits in Response to Subpoenas”.
2. **How Electronic Certified Business Records are Obtained by a User.** Any AppClose user may initiate the export of AppClose CEBR. The user selects the date range for the records, as well as the different

¹ We are not providing legal advice. An attorney should also check the rules of their own state to determine whether notice to the opposing party of the intent to use this form of business records certification is required under the state equivalent of Federal Rule 902(11) or another applicable state rule.

categories of records to be included in the export.² See **Annex A** for the types of user records that may be exported. Within a short time after the user initiates the records export, the user receives an email with a link to the CEBR export. With this link, the user can download a pdf of the CEBR export, or the user can forward the link, and any recipient of the link can download the CEBR export from the same link.

3. **How Attorneys and Courts may verify the records.** Through AppClose Pro, an attorney, other family law professional, or court official (“**Authorized Recipient**”) may request through AppClose Pro for an AppClose user to share AppClose CEBR. The AppClose user consent is given electronically. The user’s consent includes a HIPAA authorization in which the user consents to share for legal purposes any PHI that may be contained within the records, as well as any PII that may be contained within such records. The Authorized Recipient may enter the CEBR Export ID in AppClose Pro, which confirms that a CEBR export bearing that Export ID exists and is stored in the AppClose System in the form of an immutable encrypted stored version of the CEBR export. Entering an Export ID does not verify the contents of an export. The origin and integrity of a CEBR export are verified by the digital signature of AppClose, Inc. and the trusted timestamp applied to the export file itself, which any recipient of the file can check in ordinary PDF software without contacting AppClose, as described in Part A. With the appropriate AppClose user consent, the Authorized Recipient may also download the records. A Certification speaks as of the date and time the export was generated, which appear on the Certification together with the Export ID. The records AppClose maintains change over time: new records are created, and records are subject to retention periods as described in our Terms of Service, and quarantine or deletion as described in our Terms of Service and as further described below. A later export covering the same categories and date range may therefore differ from an earlier one. Each export is separately certified, is separately verifiable by its own Export ID, and remains verifiable through AppClose Pro after a later export is generated.
4. **The Certification.** The form of Business Records Certification by the AppClose Custodian of Records (the “**Certification**”) is attached as **Annex B**. The Certification states the facts required by the business-records exception to the rule against hearsay, and is designed to meet the certification requirements of Federal Rules of Evidence 902(11), 902(13) and 902(14), and their state counterparts, in jurisdictions that have adopted them (in Texas, Rule 902(10) of the Texas Rules of Evidence). AppClose CEBR are designed for use by a user or an Authorized Recipient in a court proceeding, or for other legal purposes. AppClose uses a single form of Certification for every Certified Electronic Business Records export. The Certification contains a statement of completeness that appears in every Certification and is populated by the AppClose system from the records themselves, whether or not any record within the selected categories and date range was quarantined or deleted. See “Quarantined or Deleted Records” below.
5. **Quarantined or Deleted Records.** AppClose does not edit, alter, or supplement the content of an archived records export, and an AppClose user cannot alter or delete any exportable record, including an archived record export. A user who created and shared an expense entry may withdraw it. A withdrawn expense entry remains in the records with all of its details and is displayed with a line through it. A withdrawal is an action by the user; it is not a quarantine or deletion by AppClose, and it is not counted in the statement of completeness described below.

In the limited circumstances described in our Terms of Service, AppClose may be required to quarantine a record or to delete it. A record that is **quarantined** is removed from user access but is retained in the AppClose System. A record that is **deleted** is removed from the AppClose System. AppClose takes either action only on the grounds stated in our Terms of Service — for example, where a privacy or consumer health law, a data-subject right, or legal process requires it. The decision does not originate with AppClose, and it is never the result of AppClose reviewing records to decide what should be kept.

² If the user’s Account is in Read-Only Mode, the user may still export all of the records in the Account, as described in our Terms of Service.

UNITED STATES

To quarantine or delete a record, authorized AppClose personnel decrypt the affected records, identify the record that the requirement reaches — a record that the requirement itself has specified, not one that AppClose has found by searching or reviewing records for their content — and enter a notation recording the action. This is a manual process, carried out only to satisfy the requirement. It is **not** performed by the automated processes that create, store, and export records.

The notation records the position of the affected record in the sequence of records, the date and time of that record, the account that created it, whether the record was quarantined or deleted, and the date and time of the action. The notation does not disclose the content of the record or the reason for the action. Because a notation is entered by authorized personnel rather than generated by the automated processes described above, AppClose certifies a notation as an accurate record of the action taken and of its date and time. AppClose does not certify a notation as a record generated by those automated processes.

A quarantined record continues to exist in the AppClose System, and AppClose can produce it if AppClose is compelled to do so. A deleted record does not continue to exist in the AppClose System, and AppClose does not retain a copy of it elsewhere. For a deleted record, the Certification and the Business Records Affidavit state only the facts recorded in the notation and the number and type of items deleted (for example, one message or one image). Neither states the content of a deleted record.

Where no record within the categories and date range of an export has been quarantined or deleted, the Certification and the Business Records Affidavit say so affirmatively, and nothing in this Section qualifies the certification of that export. AppClose uses a single form of Certification and a single form of Business Records Affidavit, each of which carries the same statement of completeness whether or not any record was quarantined or deleted. That statement is populated from the records themselves and gives the number of quarantined records and the number of deleted records, if any, within the selected categories and date range. AppClose does not use a separate or alternative form of Certification for records that include a quarantine or deletion notation.

6. **Access to AppClose Pro.** Access to AppClose Pro is limited to verified family law professionals and court officials. You can [request access to AppClose Pro](#).

C. BUSINESS RECORDS AFFIDAVITS IN RESPONSE TO SUBPOENAS

1. **Consider using our Certified Electronic Business Records.** Before initiating a subpoena to obtain a Business Records Affidavit with records attached, we encourage you to consider using our Electronic Certified Business Records (see Part B above), which has the following advantages over a traditional subpoena for records (*subpoena duces tecum*).
 - An AppClose Certified Electronic Business Records export can be processed electronically, which includes the required AppClose user consents. The Certified Electronic Business Records may then be obtained within minutes rather than up to 10 days for a traditional Business Records Affidavit, and **without the need to prepare and serve a subpoena** (see Service of Process below).
 - Each Certified Electronic Business Records export is encrypted and written to immutable storage at the time it is generated, together with its Export ID and a UTC timestamp. Through AppClose Pro, an Authorized Recipient can confirm that an export bearing that Export ID exists in the AppClose System. Whether the copy in the Authorized Recipient's hands is the file AppClose generated, unchanged since it was generated, is shown by the digital signature of AppClose, Inc. and the trusted timestamp on the export file itself, which can be verified in ordinary PDF software.

UNITED STATES

- While we do not provide legal advice, our Certified Electronic Business Records are designed for court admissibility based on state implementations of Federal Rules of Evidence 902(11), 902(13) and 902(14) and the hearsay exception in Rule 803(6).
- 2. ***How we search for Records in Response to Subpoenas.*** Each subpoena MUST identify the email that is associated with the account for which records are requested. We cannot locate an account by a person's name or date of birth; accounts are identified by the email address used to register them. Users may **voluntarily** enter a phone number in their profile. In such cases, we may be able to locate a user with a phone number. Nothing in this paragraph limits the records that AppClose produces in response to proper legal process.
- 3. ***Service of Process.*** We will accept and process: (a) a valid subpoena issued and served under the Texas Rules of Civil Procedure, including out-of-state subpoenas served under Texas Rules of Civil Procedure 201.3, which is based on the Uniform Interstate Depositions and Discovery Act ("UIDDA"); (b) an out-of-state subpoena sent to legal@appclose.com and **accepted by AppClose in its discretion** as described in this policy; or (c) a summons, search warrant, or subpoena from law enforcement that is valid and properly served, or sent to legal@appclose.com and accepted by AppClose in its discretion as described in this policy. 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 Registered Agents, Inc., 5900 Balcones Drive, Suite 100, Austin, TX 78731.**

Under Texas law, **service of a subpoena on a Texas resident is not effective if attempted solely by certified mail**, whether the subpoena originates from a Texas court or from out-of-state. 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 follow our recommendations below on how to submit a subpoena.

Like the UIDDA adopted in other states, to properly serve an out-of-state subpoena on a Texas business under Texas Rule 201.3, the following procedures are required:

- The out-of-state subpoena is submitted to a Texas district court clerk in the correct Texas county (in the case of AppClose, that county is Travis County)
 - The court clerk issues a Texas subpoena that incorporates the terms of the out-of-state subpoena
 - The Texas subpoena that mirrors the out-of-state subpoena is served on AppClose **under the Texas Rules of Civil Procedure**. Out-of-state parties often find it helpful to retain a Texas attorney to assist with this process.
4. ***HIPAA Authorization.*** As one of the conditions to our acceptance of service via email, 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 (legal purposes), 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. The form we use is the standard Authorization to Disclose Protected Health Information adopted by the Texas Attorney General under Section 181.154(d) of the Texas Health and Safety Code, which is attached as **Annex C**, with guidelines on how it should be completed, as

UNITED STATES

well as guidelines on how to request records. We will also accept any other authorization form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable law.³

We require this authorization as a condition of our accepting service of an otherwise proper subpoena by email, and we may waive that requirement in whole or in part, in our sole discretion, to the extent we are legally permitted to do so. Requiring the authorization is not a representation about our status under HIPAA, the Texas Medical Privacy Act, or any other health privacy law, and our response to a subpoena or court order that compels production does not depend on our receipt of an authorization.

A person who signs an authorization on behalf of a child represents that they are a legally authorized representative of that child and that no court order limits their right to access, or to authorize the disclosure of, that child's health information. As stated elsewhere in this Policy, we do not review the records, and we do not verify conservatorship, parental rights, or any court order affecting them.

5. *Types of Records Available.* We do not search the records for specific terms, or review the records in any respect. Currently, we maintain the following Exportable Records:

- chat conversations (including images)
- call detail records⁴
- check-ins (each of which records the location of the user's device at the time of the check-in, and any other location the user added), expenses, and requests
- session logs (which include the time, IP address, and mobile device operating system)⁵

The following are not categories of user records that we maintain, and they are not available in response to a subpoena:

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

If any record within the categories and date range you request has been quarantined or deleted, the records we produce will include the notation described under "Quarantined or Deleted"

³ Note that the process to generate AppClose Certified Electronic Business Records by an AppClose user includes an optional electronically obtained user consent that includes a HIPAA compliant authorization for the AppClose user's attorney or court to access (through AppClose Pro) the user designated records exports that may contain PHI and PII.

⁴ With consent of both users, calls may be recorded, and call transcripts generated. These call recordings and call transcripts are stored, and users may download them as described in the Terms of Service and Privacy Policy. Call recordings and call transcripts are not, however, certified records that we authenticate, verify, or certify as to accuracy, completeness, or origin. Such materials may be offered in various legal proceedings, but they are subject to different evidentiary standards, including chain of custody and authentication. The foundation that must be laid for admissibility of call recordings and transcripts is determined by the applicable court or other tribunal.

⁵ 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. The device identifiers that the App uses to deliver notifications and measure performance (described in Section 2.5 of the Privacy Policy) are not associated with user records and are not part of any records export. An IP address does not determine the actual person interacting with an account.

Records” in Part B above, and our Business Records Affidavit will state the number of quarantined records and the number of deleted records, if any.

See **Annex D** for guidelines on how to request available user records in your subpoena.

6. ***Recommendations on how to submit a subpoena.*** Each subpoena should identify (a) the specific types of records sought from the list above; and (b) the period for which the records are sought. See **Annex D** for guidelines on how to request records. As noted, we use the email address associated with an account to identify each account (some users **optionally** provide phone numbers). To ensure efficient processing of a subpoena, and to increase the likelihood that we will accept the subpoena via email, each civil subpoena should (a) include (or timely provide) the required properly completed and signed HIPAA authorization(s); (b) clearly describe the records requested (including the date range) from the “Types of Records Available” above; (c) 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 (d) specify an email address of an authorized recipient to which the Business Records Affidavit with records may be emailed.
7. ***Subpoena Processing Time.*** Allow up to ten days from the date that AppClose has received all required documentation. Subpoenas are often submitted without proper account user information, missing or improperly completed HIPAA authorizations, and requests for records that are not available. Once the AppClose Business Records Affidavit with records attached is complete, a pdf of such records will be emailed to the requesting law firm. If you have requested a notarized affidavit, please allow additional time.
8. ***Adverse Party Records.*** The records associated with the requesting co-parent’s 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, email addresses, or in-app session records) that are **unique** to the non-requesting co-parent’s account (“**Adverse Party Records**”). When we receive a request for Adverse Party records, we generally will not accept service via email.
9. ***Form of Business Records Affidavit.*** We use our own form of Business Records Affidavit, which is based upon the way our records are created, stored, and maintained.⁶ Records in pdf format may be searched using applicable pdf search capabilities. We use the same form of Business Records Affidavit for all subpoena responses, whether or not any record was quarantined or deleted. It contains the statement of completeness described under “Quarantined or Deleted Records” in Part B above, in the same substance as the corresponding statement in the Certification that accompanies a Certified Electronic Business Records export. Our form is available in two versions, which differ only in how it is executed: one sworn before a notary public, and one made as an unsworn declaration under penalty of perjury. We use the unsworn declaration version unless a notarized affidavit is requested or is required in the proceeding, as described in Part A above.
10. ***Attorney Considerations About Certain Data.*** When responding to a valid subpoena or court order, AppClose’ authorized technical personnel unencrypt and compile the specific data within

⁶ We may modify our form of Business Records Affidavit on a case-by-case basis to facilitate compliance with the requirements of applicable state law or the local rules of the court or other tribunal in which the records will be offered.

the date range described in the subpoena or court order. AppClose **does not** screen or otherwise review or redact the contents of the unencrypted data. We do not read the records before producing them, and we do not screen them for personally identifiable information, protected health information, privileged material, or information about children. What is withheld, redacted, or produced under seal is determined through the legal process by the parties and the tribunal, and not by AppClose. **Attorneys receiving such records should consider any applicable obligations they may have with respect to confidentiality, and sensitive information that may be contained in such records, including PII and PHI.**

11. ***Law Enforcement Subpoenas.*** Since law enforcement subpoenas are often issued with the requirement that AppClose may not notify the user of the subpoena, we do not request a HIPAA authorization in connection with a proper law enforcement subpoena. When Business Records Affidavits are provided in response to a proper subpoena from law enforcement, or in response to a court order, warrant, or other lawful legal process, the records are produced as required by that legal process. Nothing in this paragraph is a representation about our status under HIPAA, the Texas Medical Privacy Act, or any other health privacy law.
12. ***No warranties or updates.*** 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 any obligation or undertaking to provide any updates to the information transmitted.

ANNEX A

TYPES OF USER RECORDS THAT MAY BE EXPORTED

1. User selects a date range for the records export
2. Records that may be selected for export
 - a. Chats & Calls: User selects the Circle for which chat & call records are to be exported
 - b. Requests
 - i. User selects whether to export Received Requests, Sent Requests, or Both
 - ii. User selects all that apply from the following types of Requests:
 1. All
 2. Reimbursement
 3. Pickup
 4. Dropoff
 5. Swap days
 6. Other
 - c. Expenses – user selects Sent, Received, or All
 - d. Check-Ins
 - e. In-App Session Records
3. Certified vs. Uncertified Records
 - a. User selects either Uncertified Records or Certified Records.
 - b. If the User selects Certified Records, the User is directed to log in on the AppClose website. Certified Business Records can only be exported from the AppClose website.
 - c. If the User selects Uncertified Records, the User may export the Uncertified Records from within the App.

ANNEX B

FORM OF CERTIFICATION BY CUSTODIAN OF BUSINESS RECORDS

This certification is made to establish the foundation required by the business-records exception to the rule against hearsay, and is intended to satisfy Federal Rules of Evidence 902(11), 902(13) and 902(14) and their state counterparts.

1. AppClose, Inc., a Delaware corporation (the “**Company**”), provides communication and record-keeping services for parents, guardians, and related parties. I am the custodian of records for the Company, and I am familiar with the manner in which the Company creates, maintains, and stores records for the *AppClose*® mobile and web applications (“**AppClose**”).
2. In the ordinary course of the Company’s regularly conducted business activity, and at or near the time of the acts, events, and communications recorded, the *AppClose* system automatically creates, transmits, and stores electronic data reflecting user communications, exchanges, and activities. Once a record is created in *AppClose*, it is archived in the ordinary course of business as described below. Through *AppClose*, an authorized user may access and export records for that user’s account. Access to each user account is controlled by unique log-in credentials.
3. The Company does not edit, alter, or supplement the content of an archived records export, and an AppClose user cannot alter or delete any exportable record, including an archived records export. The Company quarantines or deletes a record only on the grounds stated in the Company’s Terms of Service. Any such action is reflected in the Records as described in paragraph 7.
4. Records are maintained on secure servers with Amazon Web Services (the “**Hosting Provider**”). Records are encrypted by the Company; decryption keys are controlled by the Company, and Hosting Provider personnel do not have access to the unencrypted contents. Records created in *AppClose* are accessible only to Company personnel with a need to access them to perform their duties, including when responding to lawful subpoenas and court orders.
5. When an authorized *AppClose* user initiates an *AppClose Certified Records Export*, the system retrieves the stored records as a PDF/A-2u export. Upon export of the records, the system automatically generates an Export ID, applies the digital signature of the Company, issued by a certificate authority that is a member of the Adobe Approved Trust List, and a trusted timestamp to the export file, encrypts the export file content, and stores the file content in immutable object storage, together with a UTC timestamp, in a database.
6. The attached export file(s) (the “**Records**”) are true and complete copies of records maintained by the Company in the ordinary course of its business, and it is the Company’s regular practice to make and keep such Records. The Records consist of a pdf of [NUMBER] pages from the unique AppClose user account associated with the email address [EMAIL ADDRESS]. The Records were made at or near the time of the acts, events, or communications they reflect, by – or from information transmitted by – someone with knowledge of those events and were captured contemporaneously through the Company’s automated systems. The Records were generated by an electronic process or system that ensures accurate results, and/or were copied from an electronic device, storage medium, or file, using a process that ensures an accurate copy. The *AppClose* system consistently applies the same standardized, tested process to all such records, including time-stamping, hashing, digital signing, and metadata capture, designed to ensure accuracy and integrity. The audit trail and system logs reflect that the same process was applied to the Records.
7. The Records comprise all records within the categories and date range selected for this export that were maintained by the Company at the time this export was generated. [If none: No record within those categories and that date range was quarantined or deleted.] [If any: [NUMBER] record(s) within those categories and that date range were quarantined, and [NUMBER] record(s) were deleted. Each is represented in the Records by a notation entered by authorized Company personnel recording the position of the affected record in the sequence of records, the date and time of that record, the account that created it, whether the record was quarantined or deleted, and the date and time of the action. The notation does not disclose the content of the record or the reason for the action. A notation is entered manually to satisfy a legal or regulatory requirement; it is **not** generated by the automated processes described in paragraphs 2, 5 and 6, and I certify it as an accurate record of the action taken and of its date and time and not as a record generated by those processes. A quarantined record is retained by the Company and can be produced if the Company is compelled to produce it. A deleted record is not retained; the Company can state only the facts recorded in the notation and the number and type of items deleted.] Records are subject to the retention periods stated in the Company’s Terms of Service.
8. The export of the Records was made using the same automated processes used to maintain the original data. The Records were created by a process of digital identification that accurately reproduces the data from the original electronic device, storage medium, or file. The Company does not read, screen, review, or redact records in connection with an export.
9. This certification speaks as of the date and time this export was generated, which appear below together with the Export ID. I sign this certification electronically by my typed signature below, which the *AppClose Certified Records Export* process applies under my written authorization at the time each export is generated. The export file containing this certification and the Records is also signed with the digital signature of AppClose, Inc. as described in paragraph 5 above. The digital signature identifies the Company as the source of the file and reveals any alteration made to the file after it was signed. I declare under penalty of perjury that the foregoing is true and correct.

Executed on [DATE] in Austin, Texas.

/s/ Dennis James

Dennis James

Custodian of Records

AppClose, Inc.

records@appclose.com

Export ID: _____

Generated: _____ (UTC)

ANNEX C

HIPAA AUTHORIZATION COMPLETION GUIDELINES

The following Notes apply to the attached HIPAA Authorization Form.

NOTE A: A separate completed and signed form is required for (a) the requesting co-parent; and (b) EACH minor child. By signing a form for a child, the requesting co-parent represents that they are a legally authorized representative of that child and that no court order limits their right to access, or to authorize the disclosure of, that child's health information. We do not verify conservatorship, parental rights, or any court order affecting them.

NOTE B: Insert the following: AppClose, Inc., 5000 Plaza on the Lake, Suite 300, Austin, TX 78746. Phone: 888-567-0727.

NOTE C: The recipient should be the name of the person or entity who will use the information received with the Business Records Affidavit. If the recipient is a law firm, using the name of the law firm provides authorization to that law firm's staff, agent, and subcontractors who "carry out activities and purposes permitted by this form for that organization". The "Reason for Disclosure" is "Legal Purposes".

Note D: "All health information" should be checked. The remaining categories on the form describe records created by health care providers and health plans. AppClose does not create clinical records, and does not categorize or label the content of user communications, so checking "All health information" is the selection that covers everything in an AppClose account that may constitute protected health information.

Note E: Any revocation of the permission must be sent to the Authorized Recipient. For example, if a law firm is named as the recipient, any revocation notice should be sent to the law firm. We also recommend that you insert a specific date in the "Effective Time Period" section of the form. If no date is inserted, an authorization signed for a child expires when that child reaches the age of majority.

Note F: Each form should be signed and dated by the requesting co-parent. The signatory and the Authorized Recipient should be aware that once the Authorized Recipient has the information, as noted in the form any further re-disclosure by the Authorized Recipient may no longer be protected by federal or state privacy laws and any PHI and PII that may be contained in the records should be handled accordingly. We do not provide legal advice.

The foregoing Notes are subject to the "Important Information About the Authorization to Disclose Protected Health Information" attached to the form.



AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective June 2013

Please read this entire form before signing and complete all the sections that apply to your decisions relating to the disclosure of protected health information. Covered entities as that term is defined by HIPAA and Texas Health & Safety Code § 181.001 must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing certain insurance functions, or as may be otherwise authorized by law. Covered entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws. Individuals cannot be denied treatment based on a failure to sign this authorization form, and a refusal to sign this form will not affect the payment, enrollment, or eligibility for benefits.

NAME OF PATIENT OR INDIVIDUAL

[SEE NOTE A]

Last First Middle

OTHER NAME(S) USED

DATE OF BIRTH Month Day Year

ADDRESS

CITY STATE ZIP

PHONE () ALT. PHONE ()

EMAIL ADDRESS (Optional):

I AUTHORIZE THE FOLLOWING TO DISCLOSE THE INDIVIDUAL'S PROTECTED HEALTH INFORMATION:

Person/Organization Name [SEE NOTE B]

Address

City State Zip Code

Phone () Fax ()

WHO CAN RECEIVE AND USE THE HEALTH INFORMATION?

Person/Organization Name [SEE NOTE C]

Address

City State Zip Code

Phone () Fax ()

WHAT INFORMATION CAN BE DISCLOSED? Complete the following by indicating those items that you want disclosed. The signature of a minor patient is required for the release of some of these items. If all health information is to be released, then check only the first box.

- | | | | |
|---|--|---|---|
| ☐ All health information | ☐ History/Physical Exam | ☐ Past/Present Medications | ☐ Lab Results |
| ☐ Physician's Orders | ☐ Patient Allergies | ☐ Operation Reports | ☐ Consultation Reports |
| ☐ Progress Notes | ☐ Discharge Summary | ☐ Diagnostic Test Reports | ☐ EKG/Cardiology Reports |
| ☐ Pathology Reports | ☐ Billing Information | ☐ Radiology Reports & Images | ☐ Other |

Your initials are required to release the following information:

- | | |
|--|---|
| ☐ Mental Health Records (excluding psychotherapy notes) | ☐ Genetic Information (including Genetic Test Results) |
| ☐ Drug, Alcohol, or Substance Abuse Records | ☐ HIV/AIDS Test Results/Treatment |

EFFECTIVE TIME PERIOD. This authorization is valid until the earlier of the occurrence of the death of the individual; the individual reaching the age of majority; or permission is withdrawn; or the following specific date (optional): Month Day Year

RIGHT TO REVOKE: I understand that I can withdraw my permission at any time by giving written notice stating my intent to revoke this authorization to the person or organization named under "WHO CAN RECEIVE AND USE THE HEALTH INFORMATION." I understand that prior actions taken in reliance on this authorization by entities that had permission to access my health information will not be affected.

SIGNATURE AUTHORIZATION: I have read this form and agree to the uses and disclosures of the information as described. I understand that refusing to sign this form does not stop disclosure of health information that has occurred prior to revocation or that is otherwise permitted by law without my specific authorization or permission, including disclosures to covered entities as provided by Texas Health & Safety Code § 181.154(c) and/or 45 C.F.R. § 164.502(a)(1). I understand that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by federal or state privacy laws.

SIGNATURE X [SEE NOTE F]
Signature of Individual or Individual's Legally Authorized Representative

DATE

Printed Name of Legally Authorized Representative (if applicable):

If representative, specify relationship to the individual: ☐ Parent of minor ☐ Guardian ☐ Other

A minor individual's signature is required for the release of certain types of information, including for example, the release of information related to certain types of reproductive care, sexually transmitted diseases, and drug, alcohol or substance abuse, and mental health treatment (See, e.g., Tex. Fam. Code § 32.003).

SIGNATURE X
Signature of Minor Individual

DATE

IMPORTANT INFORMATION ABOUT THE AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective June 2013

The Attorney General of Texas has adopted a standard Authorization to Disclose Protected Health Information in accordance with Texas Health & Safety Code § 181.154(d). This form is intended for use in complying with the requirements of the Health Insurance Portability and Accountability Act and Privacy Standards (HIPAA) and the Texas Medical Privacy Act (Texas Health & Safety Code, Chapter 181). **Covered Entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws.**

Covered entities, as that term is defined by HIPAA and Texas Health & Safety Code § 181.001, must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing certain insurance functions, or as may be otherwise authorized by law. (Tex. Health & Safety Code §§ 181.154(b),(c), § 241.153; 45 C.F.R. §§ 164.502(a)(1); 164.506, and 164.508).

The authorization provided by use of the form means that the organization, entity or person authorized can disclose, communicate, or send the named individual's protected health information to the organization, entity or person identified on the form, including through the use of any electronic means.

Definitions - In the form, the terms "treatment," "healthcare operations," "psychotherapy notes," and "protected health information" are as defined in HIPAA (45 CFR 164.501). "Legally authorized representative" as used in the form includes any person authorized to act on behalf of another individual. (Tex. Occ. Code § 151.002(6); Tex. Health & Safety Code §§ 166.164, 241.151; and Tex. Probate Code § 3(aa)).

Health Information to be Released - If "All Health Information" is selected for release, health information includes, but is not limited to, all records and other information regarding health history, treatment, hospitalization, tests, and outpatient care, and also educational records that may contain health information. As indicated on the form, specific authorization is required for the release of information about certain sensitive conditions, including:

- Mental health records (excluding "psychotherapy notes" as defined in HIPAA at 45 CFR 164.501).
- Drug, alcohol, or substance abuse records.
- Records or tests relating to HIV/AIDS.
- Genetic (inherited) diseases or tests (except as may be prohibited by 45 C.F.R. § 164.502).

Note on Release of Health Records - This form is not required for the permissible disclosure of an individual's protected health information to the individual or the individual's legally authorized representative. (45 C.F.R. §§ 164.502(a)(1)(i), 164.524; Tex. Health & Safety Code § 181.102). If requesting a copy of the individual's health records with this form, state and federal law allows such access, unless such access is determined by the physician or mental health provider to be harmful to the individual's physical, mental or emotional health. (Tex. Health & Safety Code §§ 181.102, 611.0045(b); Tex. Occ. Code § 159.006(a); 45 C.F.R. § 164.502(a)(1)). If a healthcare provider is specified in the "Who Can Receive and Use The Health Information" section of this form, then permission to receive protected health information also includes physicians, other health care providers (such as nurses and medical staff) who are involved in the individual's medical care at that entity's facility or that person's office, and health care providers who are covering or on call for the specified person or organization, and staff members or agents (such as business associates or qualified services organizations) who carry out activities and purposes permitted by law for that specified covered entity or person. If a covered entity other than a healthcare provider is specified, then permission to receive protected health information also includes that organization's staff or agents and subcontractors who carry out activities and purposes permitted by this form for that organization. Individuals may be entitled to restrict certain disclosures of protected health information related to services paid for in full by the individual (45 C.F.R. § 164.522(a)(1)(vi)).

Authorizations for Sale or Marketing Purposes - If this authorization is being made for sale or marketing purposes and the covered entity will receive direct or indirect remuneration from a third party in connection with the use or disclosure of the individual's information for marketing, the authorization must clearly indicate to the individual that such remuneration is involved. (Tex. Health & Safety Code §§ 181.152, .153; 45 C.F.R. § 164.508(a)(3), (4)).

Limitations of this form - This authorization form shall not be used for the disclosure of any health information as it relates to: (1) health benefits plan enrollment and/or related enrollment determinations (45 C.F.R. § 164.508(b)(4)(ii), .508(c)(2)(ii)); (2) psychotherapy notes (45 C.F.R. § 164.508(b)(3)(ii); or for research purposes (45 C.F.R. § 164.508(b)(3)(i)). **Use of this form does not exempt any entity from compliance with applicable federal or state laws or regulations regarding access, use or disclosure of health information or other sensitive personal information (e.g., 42 CFR Part 2, restricting use of information pertaining to drug/alcohol abuse and treatment), and does not entitle an entity or its employees, agents or assigns to any limitation of liability for acts or omissions in connection with the access, use, or disclosure of health information obtained through use of the form.**

Charges - Some covered entities may charge a retrieval/processing fee and for copies of medical records. (Tex. Health & Safety Code § 241.154).

Right to Receive Copy - The individual and/or the individual's legally authorized representative has a right to receive a copy of this authorization.

ANNEX D

TYPES OF RECORDS THAT ARE AVAILABLE AND HOW TO REQUEST THEM IN A SUBPOENA

The same records that a User may export as Certified or Uncertified Business Records are available in response to a Subpoena that requests a Business Records Affidavit with certified records of the requesting co-parent. To the extent that Certified Electronic Business Records satisfy your evidentiary requirements, they will be the fastest and most efficient way to obtain Certified Business Records. If for some reason, you still need to send a Subpoena and request a Business Records Affidavit, the following records are available. If any record within the categories and date range you request has been quarantined or deleted, the records will include the notation described in this Policy under “Quarantined or Deleted Records,” and the Business Records Affidavit will state the number of quarantined records and the number of deleted records, if any. If you require a notarized affidavit rather than an unsworn declaration under penalty of perjury, please say so in your subpoena or in your cover communication.

1. Identify the email address associated with the co-parent account for which the records are requested.
2. Indicate the date range for which you request the records.
3. Exportable Records that are available
 - a. Chats & Calls.
 - i. If you request chat & call records the records will show all chats and calls within the indicated date range, including the text and images associated with chats, as well as call detail records.
 - b. Requests
 - i. The following types of Requests are available (All is the default):
 1. All
 2. Reimbursement
 3. Pickup
 4. Dropoff
 5. Swap days
 6. Other
 - ii. Indicate whether the records should include Received Requests, Sent Requests, or Both (both is the default)
 - c. Expenses
 - i. The following expense records are available: Sent, Received, or All (All is the default)
 - d. Check-Ins
 - e. In-App Session Records