CAPLAW FAQ

A series of common legal questions and answers for the CAA network

Privacy Rights of CAA Clients

By Jonathan Cohen, Esq.
December 2021

A community action agency (CAA) cannot serve its clients without gathering important details about them. Information provided by clients forms the basis for key decisions about program eligibility and the provision of services, and allows the agency to communicate better with those they serve. The information shared with a CAA often includes sensitive and personal data that is not publicly available. Thus, the CAA must understand and respect the privacy rights that clients have in their information. The CAA's processes for retaining that information and its policies governing the disclosure of such data must safeguard these privacy rights to minimize a CAA's legal exposure when handling sensitive and confidential information.

CAPLAW developed this FAQ to assist CAAs as they navigate complex client privacy issues. It includes common questions on the topic and offers answers that CAAs can use to comply with applicable laws and regulations. For additional information about these issues, please see the "Conversations with CAPLAW" session, Privacy Rights of Clients.

TABLE OF CONTENTS

GENERAL CONSIDERATIONS

1. What is client information?

"Client information" broadly describes information provided by clients or potential clients to a CAA for purposes of applying for and obtaining services offered by the agency. The type of information collected varies by CAA and often depends on applicable program funding source requirements. Client information may include a client's name, address, date of birth, phone number, email address, income, Social Security number, government-issued ID number, and bank account number. It also may include the image or voice of a client as captured in print, on video or in an audio file. Various funding sources and program rules may define protected client information differently. Generally the Office of Management and Budget's (OMB) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) includes definitions of "personally identifiable information" and "protected personally identifiable information" that may apply in the absence of funding source rules.[1]

2. What rights do clients have in their information?

In general, clients have privacy rights in the information they provide to a CAA, so an agency should assume that all client information provided to it must be kept confidential, unless disclosure is authorized by the client or otherwise required by applicable law (such as client information that a court orders a CAA to produce via a subpoena). Federal and state laws and regulations related to the privacy of information, including funding source requirements, may contain specific requirements about how a CAA should collect, retain, and safeguard client information. As a best practice, a CAA should obtain client consent before it discloses or shares any client information, both internally and with third parties. This includes obtaining consent before disclosing any non-public client information contained in federally-required reports.

3. Do we need to notify clients of their privacy rights?

Since funding sources and state laws often require providers to notify clients of their privacy rights, it is generally recommended that a CAA do so. Funding source requirements are found in the laws and regulations that govern the programs, and/or within the grant agreements and contracts between awarding agencies and CAAs. Requirements around the timing and details of these notifications vary by funding source. For example, the Head Start Performance Standards require that parents receive annual, written notice from the program about their privacy rights related to the personally identifiable information (PII) in their child's records.[2]

States may also have laws that require businesses to notify individuals of their data collection practices and what types of personal information they collect.[3] In some cases, these laws give individuals the right to know the personal information being collected, as well as to request businesses to delete the information. CAAs should work with a state law attorney to determine the applicability of these state laws with respect to the CAA's client information.

4. How do we notify clients of their privacy rights?

CAAs can notify clients about their privacy rights as part of their applications for CAA services, as well as when the CAA asks a client to sign a consent to release information form with the agency. Some programs also have specific notification requirements. For example, Head Start requires that programs provide an annual written notice to Head Start parents, which must include a description of the types of PII that may be disclosed, to whom it may be disclosed, and what may constitute a necessary reason for the disclosure without parental consent.[4]

DATA COLLECTION/INTAKE

5. What types of information can our CAA collect from clients?

In general, a CAA can collect whatever information it wants from clients, but it should obtain a consent from each client prior to using or disclosing that information. Some funding sources may limit what information a CAA needs from a client for purposes of receiving funded services. A CAA should refrain from collecting more information than it needs

because, in general, applicable laws require that information received be protected. A CAA that only collects information that it needs will have fewer obligations, and subsequently, fewer potential liabilities.

When determining what types of client information to collect, including any information not required for participation in the program, a CAA should be mindful of the data privacy and confidentiality obligations they may have with respect to such information. For example, some state laws require that organizations have written information security policies covering the organization's collection, use, and storage of certain types of PII. If a CAA collects protected information, it may trigger application of these requirements and mandate a certain level of security.

6. What types of information should our CAA not collect from clients?

As noted in earlier questions, a CAA is not necessarily prohibited from collecting information from clients; rather the ability to use, or the obligation to protect, the information provided often depends on the nature of that information. There are increased sensitivities, and in some cases, legal requirements, around asking for certain types of information, including information about criminal history, substance abuse treatment, and health. A CAA should check applicable laws and regulations before requesting these types of information. Further, while a CAA likely may ask clients for demographic information such as race, ethnicity, and gender, it is best practice to make these questions optional, unless otherwise required by a funding source.

7. At what point should our CAA collect client information?

A CAA should ask for and collect client information at the time of client intake since that is typically when consents and releases are signed. If a CAA asks for additional information at a later date, it should confirm that the current consents and releases cover the information obtained at that time and, if they do not, considering entering into new ones that do.

8. How should our CAA serve clients who refuse to provide the information we request?

If a client refuses to provide information requested by the CAA, the agency's ability to serve the client will depend on the reason(s) why the CAA needs the information. In making these decisions, a CAA should determine if the information requested is required by law, regulation, or a funding source contract or policy for the particular benefits sought or to meet a reporting obligation and if alternate information may be used to meet those requirements.

If information is necessary to make a decision about program eligibility as required by a funding source, then the CAA should see if funding source rules contain any flexibility to permit clients to provide alternative sources of information. If they do not, and if there is no other way for the CAA to make the required decision without the information requested, the CAA may have no choice but to deny services to the client.

If the information is requested to enable the CAA to produce reports, the CAA should also consider the availability of other data and whether the reports are required as a condition of receiving funding.

CLIENT RELEASES

9. What is a release of information form, and can our CAA ask clients to sign one?

A release of information form typically authorizes the CAA to use and release client information for certain, specified purposes. CAAs may ask clients to sign a release of information form. Usually they do so at the time that client information is collected. CAAs that collect release forms at the time of intake may take different approaches to the scope of the information covered as well as the extent of the release authorized. While CAAs often want to include all potential releases of information in one form, a CAA should always check the release each time it wants to use client-specific information. Some releases of information not covered by more general release forms may require more specific release of information forms be signed at a later date. If a CAA is unsure whether information is covered in an existing release form, it should obtain another form prior to releasing that information.

10. What should our CAA include on its release of information forms?

A release of information form should specify the information being collected, how it will be used, to whom it will be disclosed and whether it will be shared internally across its programs and departments or with external parties. The form should note the CAA's commitment to the privacy of client information and state that client information shall not be released beyond the scope of the form. It must include language indicating that consent to release information is optional and not a requirement for clients to receive CAA services, and that consent may be withdrawn at any time with respect to future releases of information. The form should be signed and dated by the client.

Some release forms include a general disclaimer which typically consists of broad language such as "the information provided may be used for particular purposes, and may be disclosed to parties at a later date." These disclaimers are not sufficient, as they do not provide adequate notice to the client and should not be used in place of obtaining the client's written consent to use and disclose their non-public information in specified ways. If a CAA needs to disclose client information in a manner that deviates from the initial release of information form, it should ask the client to sign another release of information that covers the types of disclosures sought.

11. Do release forms expire?

If the release form does not specify an end date, it does not expire. To ensure CAAs can continue to use the information collected, release of information forms should not include an end date. However, some laws and regulations require releases to include an expiration date so that organizations must periodically request and obtain client consent to continue sharing information. For example, Health Insurance Portability and Accountability Act (HIPAA) authorizations must include either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure (e.g., "one year from the date the Authorization is signed," "upon the minor's age of majority," or "upon termination of enrollment in the health plan").

12. Must our CAA obtain a client's consent to release information in writing?

A CAA should obtain a client's consent to release information in writing prior to sharing information. This eliminates any ambiguity over whether the client consented to the release of information, and can help safeguard the organization from future liability. In some circumstances when a client's prior written consent to release information has not been obtained, however, a CAA may seek to disclose information to a third party with the client present (either physically in-person or via electronic means, such as by phone or video conference), and the CAA may validly request the client's verbal consent to share client information with the third party.

SHARING CLIENT INFORMATION WITHIN THE CAA

13. Why would a CAA want to share client information within our organization?

A CAA may want to share client information internally for a number of reasons, including to:

- Administer the program through which they are being served (e.g., to prepare fiscal reports, make payments to clients or their landlords);
- Prepare reports required by funding sources (e.g., reports to our state CSBG office on program deliverables and outcomes);
- Refer clients to and determine eligibility for other programs;
- Include client information in the organization's data warehouse, which is used for reporting and internal referral purposes;
- Update the organization's mailing list;
- Feature them in impact stories or the organization's print and online publications and social media.[5]

14. Can we share client information within our own organization?

A CAA may share client information internally across departments or programs but may be required by funding source rules and applicable state laws to obtain the client's consent before doing so. Thus, it is generally recommended that a CAA that plans to share client information internally obtain written consents from clients. This can be done via a general release of information form, but should specify that the client consents to disclosures of information to the CAA's other departments or programs. The consent should also inform clients about the purpose of such disclosures (e.g., to determine whether the client is eligible for other programs and provide referrals to additional services offered by the CAA).

SHARING CLIENT INFORMATION WITH THIRD PARTIES

15. Can our CAA share client information with partner agencies to help coordinate services?

Yes, a CAA may share any information the client has consented to sharing, unless funding source rules prohibit it. A CAA that shares client information with a partner organization should put in place a data sharing agreement that clearly defines how information is

shared and the safeguards that must be in place to protect it. In some cases, a data sharing agreement may be required by the funding source or the grant agreement. For example, the Head Start Performance Standards require that written agreements with third parties include procedures to protect PII that are reviewed annually and updated if necessary.[6]

16. How should our CAA respond to requests from third parties for client data?

In general, a CAA should limit the client information it provides to third parties to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Responses to requests for client data will vary, depending on the third party and the nature of the request. If a request for data or information contains confidential information of multiple clients or individuals, a CAA must, in general, obtain consent from all of the individuals whose information is subject to the request prior to its release.

Considerations for the following specific requests include:

- Police/immigration officials. If the police or an immigration officer requests information about a client, the CAA should not assume it must provide it to them. Instead, the CAA should inform the officer that a client's data is subject to numerous confidentiality requirements and that the officers must either provide a subpoena for the data or, if they intend to search the organization, a warrant. If the police or immigration officer produces one of those documents, the CAA should ask an attorney to review the contents of the subpoena or warrant before providing the information, to ensure they are properly issued and to determine the scope of the information requested.

- Subpoenas and court orders. If a CAA receives a subpoena or court order requesting client data, it should first consult an attorney for advice on whether it should provide all or some of the information subpoenaed.

- Researchers. A recommended practice is to obtain a client's prior written consent before providing identifying personal data to researchers. While consents may not always be required, a CAA should verify the rules that permit release without consent because they often place limits on when and what information may be released. For example, under the Head Start Performance Standards, information from child records may be disclosed without parental consent to officials within the program, acting for the program, or from a federal or state entity, to conduct a study to improve child and family outcomes if additional requirements are met.[7] If a CAA may disclose client information without consent, it should (and in some cases may be required to) inform the client of the circumstances under which such disclosures are permitted.[8]

- Family members. Parents or guardians whose legal custody of a child is not contested have a right to their minor child's records and data. Other family members generally do not have a right to a client's information unless the client has given written consent to an organization to provide that information to the family member.

- EMS in event of emergency. Generally, there are exceptions to privacy laws permitting disclosures of otherwise protected personal information to enable emergency personnel to deliver medical and other emergency services.

- Subgrantees, contractors and vendors. A CAA should include and review privacy and confidentiality language in its contracts with subgrantees, contractors, and vendors. This language will determine whether and the extent to which client information may be disclosed.

- Public records. Public CAAs and some nonprofit CAAs are subject to state public records or sunshine laws. These laws vary by state and provide public access to certain records retained by these CAAs. If a CAA receives a request for public records or information, it should consult with a state attorney prior to disclosing any client information requested to determine whether its state public records law applies, and if so, what information is considered public under the law. Many state laws limit what PII may be disclosed in response to a public records request, and what information may be covered by an exception to disclosure or could be redacted.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

17. When might our CAA be covered by HIPAA?

A CAA should not assume it is covered by HIPAA, nor should it assume that all health-related information it collects is covered by HIPAA. HIPAA only applies to "covered entities" and "business associates."[9]

A CAA is a "covered entity" if it is a healthcare provider that transmits health information in electronic form with health plans in connection with certain standard transactions. If a CAA thinks it might be a covered entity, it should first determine whether its operations involve billing health plans. For example, if a CAA provides services that it bills to Medicaid, the Children's Health Insurance Program (CHIP), Medicare, or private health plans, it is covered by HIPAA.

A CAA is a "business associate" if it has a written business associate agreement with another HIPAA covered entity or business associate. These agreements can be with state agencies, nonprofit organizations, or for-profit entities, and they govern the creation, receipt, maintenance, or transmission of protected health information on behalf of a HIPAA covered entity or business associate. As a best practice, if a CAA sees the term "business associate" in any contract, it should not assume that it is a business associate and should not automatically sign it. A CAA should seek assistance from an attorney who can counsel the agency on whether it is a business associate. Given the potential liability associated with noncompliance with HIPAA, a CAA does not want to sign a business associate agreement if it does not have to.

DATA BREACHES

18. When does our CAA need to notify clients about data breaches?

Notification requirements for data breaches will depend on what state a CAA is in, what information is compromised as part of the data breach, and what laws apply to that information. Most states have laws that require notification of breaches of certain types

of data. This usually includes disclosures of a client's first name or first initial and last name, plus one or more of the following: (i) Social Security number; (ii) driver's license number or state-issued ID card number; or (iii) account number, credit card number, or debit card number combined with any security code, access code, PIN or password needed to access an account. A small number of states also require notification of breaches of an individual's date of birth. In most cases, a breach involving just names or email addresses will not require notification. However, if HIPAA or another similarly stringent rule or regulation applies, a more formal breach notification may be required. Such notices must comply with the applicable processes and requirements of the laws requiring notification.

19. Do our insurance policies cover data breaches?

CAAs may purchase insurance that covers the costs associated with data breaches. Generally referred to as "cyber-liability insurance", such policies may protect a covered organization from a range of losses, including data breaches and theft or destruction of data. The scope of coverage and costs of these policies vary depending on a CAA's location and size, as well as other factors. CAAs reviewing their cyber insurance policies should carefully consider the types of coverage available, including liability to third parties for data breaches, remediation costs to respond to a breach (such as offering credit monitoring to affected individuals), reimbursement for ransom and related expenses arising from cyber extortion, and coverage for fines and penalties imposed by law or regulation as a result of the data breach.

POLICIES AND TRAINING

20. How should we approach incorporating client privacy protections in our organization?

A CAA should think holistically about the ways in which a client's privacy rights may arise and impact operations. No one-off practice or procedure can account for the numerous ways in which a client's privacy rights may be implicated, so a CAA should consider the protection of client privacy in all of the programs and areas in which it may arise at the agency, and ensure that existing policies and practices in those areas include language that incorporates applicable federal and state requirements. A CAA should work with an attorney licensed in its state when developing and reviewing these policies.

21. What organizational policies may address client privacy?

As part of the holistic approach that CAAs take to protect client privacy, CAAs should review the following policies and ensure they address the agency's protection of client privacy:

- Internal program procedures– e.g., Head Start policy/program manual
- Client release of information for applications for services
- Data sharing agreements with third parties
- Vendor/consultant contract language
- Staff and board confidentiality requirements/agreements (which may be found in employee handbooks/board policies and procedures)
- Communications policy
- Record Retention policy

- Remote Work policy
- Confidentiality policy
- Policy for photographing/recording clients
- Social media policy
- Website privacy policy

A CAA may develop and implement a general policy for client information that reflects requirements around data privacy and protection, and includes centralized processes for handling requests for client data from third parties. Where applicable, the development of these policies and procedures should involve an attorney. However, given the variability of requirements for certain programs, such as Head Start or WIC, a CAA may need to implement client privacy policies at a program level to comply with more particular or stringent requirements.

22. What kind of training would a CAA provide and to whom?

A CAA could provide training to staff and volunteers about their obligations to protect and keep confidential client information when they first join the organization, and periodically after that. This can be done in multiple stages, including at the general staff or volunteer orientation, and later within the specific program(s) in which they will be working. In addition, subsequent trainings could be provided to communicate changes in client privacy rules and policies, and data protection practices and technology.

23. Does CAPLAW have any sample policies or additional resources?

While CAPLAW has not developed a sample policy that covers all client privacy issues discussed in this FAQ, a CAA may consider the following sample CAPLAW policies as part of its holistic approach to protecting client information:

- Sample Record Retention policy
- Sample Remote Work policy
- Sample Social Media policy

The following CAPLAW resources also provide information related to protecting client privacy:

- Is Your Head in the Cloud? Contemplating Cloud Computing for Community Action Agencies
- 10 Data Security Tips to Protect Your CAA
- Can I Disclose This Information? Complying with Confidentiality and Disclosure Requirements

ENDNOTES

[1] The Uniform Guidance defines "personally identifiable information" as:

> *[I]nformation that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.*

The Uniform Guidance defines "protected personally identifiable information" as:

> *[A]n individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed. See also the definition of Personally Identifiable Information (PII) in this section.*

See 2 C.F.R. § 200.1.

[2] 45 C.F.R. § 1303.22(e).

[3] See, for example, the California Consumer Privacy Act of 2018, which states:

> *A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.*

CA CIVIL § 1798.100(b).

[4] 45 C.F.R. § 1303.22(e).

[5] CAAs should obtain a media release permitting the client's image/voice to be used for the specified purposes.

[6] 45 C.F.R. § 1303.22(d).

[7] 45 C.F.R. § 1303.22(c).

[8] Under the Head Start Performance Standards, Head Start programs must notify parents of their privacy rights to their children's records in writing, and must describe the reasons for disclosing information without parental consent. 45 C.F.R. § 1303.22(e).

[9] In general, if a CAA has a health insurance plan for employees, that plan is mostly covered by HIPAA. However, most of the HIPAA obligations related to the plan lie with the insurer rather than the CAA.

This publication is part of the Community Services Block Grant (CSBG) Legal Training and Technical Assistance (T/TA) Center. It was created by Community Action Program Legal Services, Inc. (CAPLAW) in the performance of the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Community Services Cooperative Agreement – Award Number 90ET0482-02. Any opinion, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Health and Human Services, Administration for Children and Families.